

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-84339

(43) 公開日 平成10年(1998) 3月31日

(51) Int.Cl. ⁶	識別記号	庁内整理番号	F I	技術表示箇所
H 0 4 L 9/20			H 0 4 L 9/00	6 5 3
G 0 9 C 1/00	6 1 0	7259-5 J	G 0 9 C 1/00	6 1 0 D
H 0 4 L 9/08			H 0 4 L 9/00	6 0 1 C

審査請求 未請求 請求項の数30 O L (全 45 頁)

(21) 出願番号 特願平8-236862

(22) 出願日 平成8年(1996) 9月6日

(71) 出願人 000004226

日本電信電話株式会社

東京都新宿区西新宿三丁目19番2号

(72) 発明者 高木 剛

東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内

(72) 発明者 内藤 昭三

東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内

(74) 代理人 弁理士 三好 秀和 (外1名)

(54) 【発明の名称】 ストリーム暗号による通信方法、ならびに通信システム

(57) 【要約】

【課題】 ストリーム暗号における秘密鍵である乱数を共有するための処理量を削減し、高速な暗号化通信を行う。

【解決手段】 乱数共有化手段21により送信装置31と受信装置51との間で、予め乱数 $R[j]$ ($1 \leq j \leq k$) を共有する。平文メッセージを $M[i]$ ($1 \leq i \leq N$)、暗号化メッセージ $C[i]$ ($1 \leq i \leq N$)とする。送信装置31は、以下の式によりビット毎の暗号化を行う。(+)は排他的論理和である。

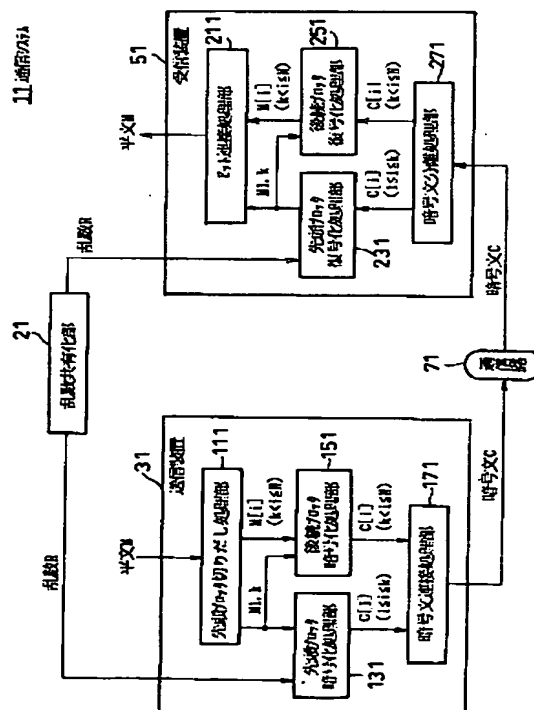
$$C[i] \equiv R[i] (+) M[i] \quad (1 \leq i \leq k \text{ のとき})$$

$$C[i] \equiv M[i-k] (+) M[i] \quad (k < i \text{ のとき})$$

受信装置51は、共有乱数 R を使って以下の式により復号化する。

$$M[i] \equiv R[i] (+) C[i] \quad (1 \leq i \leq k \text{ のとき})$$

$$M[i] \equiv M[i-k] (+) C[i] \quad (k < i \text{ のとき})$$



1

【特許請求の範囲】

【請求項 1】送信装置と受信装置との間で、予め所定ビット長を有する乱数を共有し、

前記送信装置は、

通信メッセージの先頭ビットから前記乱数の所定ビット長に等しい長さの各ビットにより構成された第 1 の領域の通信メッセージに対しては、これらの各ビットと、前記乱数の先頭ビットから所定ビット長までの各ビットと、をそれぞれ互いに排他的論理和演算することにより、第 1 の暗号化メッセージを生成し、

前記乱数の所定ビット長を超える前記通信メッセージの各ビットから構成された第 2 の領域の通信メッセージに対しては、これらの各ビットと、該ビット位置から前記乱数の所定ビット長を減じたビット位置の前記通信メッセージの各ビットと、をそれぞれ互いに排他的論理和演算することにより、第 2 の暗号化メッセージを生成し、第 1 及び第 2 の暗号化メッセージを前記送信装置から前記受信装置へ通信し、

前記受信装置は、

第 1 の暗号化メッセージに対しては、これらの各ビットと、前記乱数の先頭ビットから所定ビット長までの各ビットと、をそれぞれ互いに排他的論理和演算することにより、第 1 の暗号化メッセージから第 1 の領域の通信メッセージを復号化し、

第 2 の暗号化メッセージに対しては、これらの各ビットと、該ビット位置から前記乱数の所定ビット長を減じたビット位置の前記通信メッセージの各ビットと、をそれぞれ互いに排他的論理和演算することにより、第 2 の暗号化メッセージから第 2 の領域の通信メッセージを復号化することを特徴とするストリーム暗号による通信方法。

【請求項 2】送信装置と受信装置との間で、公開鍵配送法により、予め所定ビット長を有する乱数を共有し、

前記送信装置は、

通信メッセージの先頭ビットから前記乱数の所定ビット長に等しい長さの各ビットにより構成された第 1 の領域の通信メッセージに対しては、これらの各ビットと、前記乱数の先頭ビットから所定ビット長までの各ビットと、をそれぞれ互いに排他的論理和演算することにより、第 1 の暗号化メッセージを生成し、

前記乱数の所定ビット長を超える前記通信メッセージの各ビットから構成された第 2 の領域の通信メッセージに対しては、これらの各ビットと、該ビット位置から前記乱数の所定ビット長を減じたビット位置の前記通信メッセージの各ビットと、をそれぞれ互いに排他的論理和演算することにより、第 2 の暗号化メッセージを生成し、第 1 及び第 2 の暗号化メッセージを前記送信装置から前記受信装置へ通信し、

前記受信装置は、

第 1 の暗号化メッセージに対しては、これらの各ビット

(2)

特開平 10-84339

2

と、前記乱数の先頭ビットから所定ビット長までの各ビットと、をそれぞれ互いに排他的論理和演算することにより、第 1 の暗号化メッセージから第 1 の領域の通信メッセージを復号化し、

第 2 の暗号化メッセージに対しては、これらの各ビットと、該ビット位置から前記乱数の所定ビット長を減じたビット位置の前記通信メッセージの各ビットと、をそれぞれ互いに排他的論理和演算することにより、第 2 の暗号化メッセージから第 2 の領域の通信メッセージを復号化することを特徴とするストリーム暗号による通信方法。

【請求項 3】送信装置と受信装置との間で、公開鍵暗号による暗号化通信により、予め所定ビット長を有する乱数を共有し、

前記送信装置は、

通信メッセージの先頭ビットから前記乱数の所定ビット長に等しい長さの各ビットにより構成された第 1 の領域の通信メッセージに対しては、これらの各ビットと、前記乱数の先頭ビットから所定ビット長までの各ビットと、をそれぞれ互いに排他的論理和演算することにより、第 1 の暗号化メッセージを生成し、

前記乱数の所定ビット長を超える前記通信メッセージの各ビットから構成された第 2 の領域の通信メッセージに対しては、これらの各ビットと、該ビット位置から前記乱数の所定ビット長を減じたビット位置の前記通信メッセージの各ビットと、をそれぞれ互いに排他的論理和演算することにより、第 2 の暗号化メッセージを生成し、第 1 及び第 2 の暗号化メッセージを前記送信装置から前記受信装置へ通信し、

前記受信装置は、

第 1 の暗号化メッセージに対しては、これらの各ビットと、前記乱数の先頭ビットから所定ビット長までの各ビットと、をそれぞれ互いに排他的論理和演算することにより、第 1 の暗号化メッセージから第 1 の領域の通信メッセージを復号化し、

第 2 の暗号化メッセージに対しては、これらの各ビットと、該ビット位置から前記乱数の所定ビット長を減じたビット位置の前記通信メッセージの各ビットと、をそれぞれ互いに排他的論理和演算することにより、第 2 の暗号化メッセージから第 2 の領域の通信メッセージを復号化することを特徴とするストリーム暗号による通信方法。

【請求項 4】送信装置から受信装置へ、公開鍵暗号により暗号化した乱数と、ストリーム暗号化した通信メッセージと、を送るストリーム暗号による通信方法であつて、

前記送信装置は、

所定ビット長を有する乱数を発生させ、該乱数を受信装置の公開鍵により暗号化して、暗号化乱数を生成し、通信メッセージの先頭ビットから前記乱数の所定ビット

3

長に等しい長さの各ビットにより構成された第1の領域の通信メッセージに対しては、これらの各ビットと、前記乱数の先頭ビットから所定ビット長までの各ビットと、をそれぞれ互いに排他的論理和演算することにより、第1の暗号化メッセージを生成し、前記乱数の所定ビット長を超える前記通信メッセージの各ビットから構成された第2の領域の通信メッセージに対しては、これらの各ビットと、該ビット位置から前記乱数の所定ビット長を減じたビット位置の前記通信メッセージの各ビットと、をそれぞれ互いに排他的論理和演算することにより、第2の暗号化メッセージを生成し、前記暗号化乱数と第1および第2の暗号化メッセージとを接続して前記送信装置から前記受信装置へ通信し、前記受信装置は、前記暗号化乱数を自らの秘密鍵により復号化して乱数を生成し、第1の暗号化メッセージに対しては、これらの各ビットと、前記乱数の先頭ビットから所定ビット長までの各ビットと、をそれぞれ互いに排他的論理和演算することにより、第1の暗号化メッセージから第1の領域の通信メッセージを復号化し、第2の暗号化メッセージに対しては、これらの各ビットと、該ビット位置から前記乱数の所定ビット長を減じたビット位置の前記通信メッセージの各ビットと、をそれぞれ互いに排他的論理和演算することにより、第2の暗号化メッセージから第2の領域の通信メッセージを復号化することを特徴とするストリーム暗号による通信方法。

【請求項5】前記乱数のビット数は、前記公開鍵暗号により1度に暗号化可能なビット数を超えるビット数であり、前記乱数が複数の部分に分割されてそれぞれ暗号化され、復号化後に1つの乱数として接続されて暗号化メッセージの復号化に利用されることを特徴とする請求項3または請求項4に記載のストリーム暗号による通信方法。

【請求項6】それぞれ乱数発生器を備えた送信装置と受信装置との間で、公開鍵暗号を用いる暗号化通信により、乱数発生アルゴリズム及びまたは乱数の初期値を共有することにより、双方の乱数発生器から所定ビット長の同一の乱数を発生させ、前記送信装置は、通信メッセージの先頭ビットから前記乱数の所定ビット長に等しい長さの各ビットにより構成された第1の領域の通信メッセージに対しては、これらの各ビットと、前記乱数の先頭ビットから所定ビット長までの各ビットと、をそれぞれ互いに排他的論理和演算することにより、第1の暗号化メッセージを生成し、前記乱数の所定ビット長を超える前記通信メッセージの各ビットから構成された第2の領域の通信メッセージに対しては、これらの各ビットと、該ビット位置から前記

(3)

特開平10-84339

4

乱数の所定ビット長を減じたビット位置の前記通信メッセージの各ビットと、をそれぞれ互いに排他的論理和演算することにより、第2の暗号化メッセージを生成し、第1及び第2の暗号化メッセージを前記送信装置から前記受信装置へ通信し、前記受信装置は、第1の暗号化メッセージに対しては、これらの各ビットと、前記乱数の先頭ビットから所定ビット長までの各ビットと、をそれぞれ互いに排他的論理和演算することにより、第1の暗号化メッセージから第1の領域の通信メッセージを復号化し、第2の暗号化メッセージに対しては、これらの各ビットと、該ビット位置から前記乱数の所定ビット長を減じたビット位置の前記通信メッセージの各ビットと、をそれぞれ互いに排他的論理和演算することにより、第2の暗号化メッセージから第2の領域の通信メッセージを復号化することを特徴とするストリーム暗号による通信方法。

【請求項7】前記送信装置及び受信装置にそれぞれ備えられた乱数発生器から、発生される乱数の周期を超えて、それぞれ乱数を取り出すことを特徴とする請求項6に記載のストリーム暗号による通信方法。

【請求項8】通信メッセージの先頭から所定のビット長を第1の領域の通信メッセージとし、前記通信メッセージの所定のビット長を超える部分を第2の領域の通信メッセージとする通信メッセージの分割を行い、第1の領域の通信メッセージに対しては公開鍵暗号により、第2の領域の通信メッセージに対してはストリーム暗号により、それぞれ送信装置から受信装置へ通信する通信方法であって、

前記送信装置は、第1の領域の通信メッセージを受信装置の公開鍵により暗号化して、第1の暗号化メッセージを生成し、第2の領域の通信メッセージに対しては、これらの各ビットと、該ビット位置から前記第1の領域の通信メッセージのビット長を減じたビット位置の前記通信メッセージの各ビットと、をそれぞれ互いに排他的論理和演算することにより、第2の暗号化メッセージを生成し、前記第1および第2の暗号化メッセージを接続して前記送信装置から前記受信装置へ通信し、前記受信装置は、自らの秘密鍵により、前記第1の暗号化メッセージから第1の領域の通信メッセージを復号化し、前記第2の暗号化メッセージの各ビットに対しては、これらの各ビットと、該ビット位置が対応する前記通信メッセージのビット位置から前記所定のビット長を減じたビット位置の復号化された通信メッセージの各ビットと、をそれぞれ互いに排他的論理和演算することにより、第2の暗号化メッセージから第2の領域の通信メッセージを復号化する、

50

5

ことを特徴とするストリーム暗号による通信方法。

【請求項 9】前記第 1 の領域の通信メッセージのビット数は、前記公開鍵暗号により 1 度に暗号化可能なビット数を超えるビット数であり、それぞれ複数回の暗号化及び復号化によって第 1 の領域の通信メッセージの暗号化及び復号化が行われることを特徴とする請求項 8 に記載のストリーム暗号による通信方法。

【請求項 10】送信装置と受信装置との間で、予め所定ビット長を有する乱数を共有し、
前記送信装置は、前記乱数の所定ビット長と等しいブロック長を有する転置情報を前記受信装置の公開鍵により暗号化した暗号化転置情報を生成し、
通信メッセージの先頭ビットから前記乱数の所定ビット長に等しい長さの各ビットにより構成された第 1 の領域の通信メッセージに対しては、前記転置情報に基づいて、これらの各ビットを前記乱数の所定ビット長と等しいブロック長の転置を施した転置メッセージの各ビットと、前記乱数の先頭ビットから所定ビット長までの各ビットと、をそれぞれ互いに排他的論理和演算することにより、第 1 の暗号化メッセージを生成し、
前記乱数の所定ビット長を超える前記通信メッセージの各ビットから構成された第 2 の領域の通信メッセージに対しては、前記転置情報に基づいて、これらの各ビットを前記転置のブロック長の単位毎に転置を施した転置メッセージの各ビットと、前記通信メッセージの該ビット位置から前記乱数の所定ビット長を減じたビット位置の前記通信メッセージの各ビットと、をそれぞれ互いに排他的論理和演算することにより、第 2 の暗号化メッセージを生成し、
前記暗号化転置情報と第 1 の暗号化メッセージと第 2 の暗号化メッセージとを接続して前記送信装置から前記受信装置へ通信し、
前記受信装置は、
自らの秘密鍵により前記暗号化転置情報から転置情報を復号化し、
第 1 の暗号化メッセージに対しては、これらの各ビットと、前記乱数の先頭ビットから所定ビット長までの各ビットと、をそれぞれ互いに排他的論理和演算して得られた転置メッセージに前記転置の逆写像の転置を施して第 1 の領域の通信メッセージを復号化し、
第 2 の暗号化メッセージに対しては、これらの各ビットと、該ビット位置から前記乱数の所定ビット長を減じたビット位置の前記通信メッセージの各ビットと、をそれぞれ互いに排他的論理和演算して得られた転置メッセージに前記転置の逆写像の転置を施して第 2 の領域の通信メッセージを復号化することを特徴とするストリーム暗号による通信方法。

【請求項 11】送信装置と受信装置との間で、公開鍵配送法により、予め所定ビット長を有する乱数を共有し、
前記送信装置は、前記乱数の所定ビット長と等しいプロ

(4)

特開平 10-84339

6

ック長を有する転置情報を前記受信装置の公開鍵により暗号化した暗号化転置情報を生成し、
通信メッセージの先頭ビットから前記乱数の所定ビット長に等しい長さの各ビットにより構成された第 1 の領域の通信メッセージに対しては、前記転置情報に基づいて、これらの各ビットを前記乱数の所定ビット長と等しいブロック長の転置を施した転置メッセージの各ビットと、前記乱数の先頭ビットから所定ビット長までの各ビットと、をそれぞれ互いに排他的論理和演算することにより、第 1 の暗号化メッセージを生成し、
前記乱数の所定ビット長を超える前記通信メッセージの各ビットから構成された第 2 の領域の通信メッセージに対しては、前記転置情報に基づいて、これらの各ビットを前記転置のブロック長の単位毎に転置を施した転置メッセージの各ビットと、前記通信メッセージの該ビット位置から前記乱数の所定ビット長を減じたビット位置の前記通信メッセージの各ビットと、をそれぞれ互いに排他的論理和演算することにより、第 2 の暗号化メッセージを生成し、
前記暗号化転置情報と第 1 の暗号化メッセージと第 2 の暗号化メッセージとを接続して前記送信装置から前記受信装置へ通信し、
前記受信装置は、
自らの秘密鍵により前記暗号化転置情報から転置情報を復号化し、
第 1 の暗号化メッセージに対しては、これらの各ビットと、前記乱数の先頭ビットから所定ビット長までの各ビットと、をそれぞれ互いに排他的論理和演算して得られた転置メッセージに前記転置の逆写像の転置を施して第 1 の領域の通信メッセージを復号化し、
第 2 の暗号化メッセージに対しては、これらの各ビットと、該ビット位置から前記乱数の所定ビット長を減じたビット位置の前記通信メッセージの各ビットと、をそれぞれ互いに排他的論理和演算して得られた転置メッセージに前記転置の逆写像の転置を施して第 2 の領域の通信メッセージを復号化することを特徴とするストリーム暗号による通信方法。

【請求項 12】送信装置と受信装置との間で、公開鍵暗号による暗号化通信により、予め所定ビット長を有する乱数を共有し、
前記送信装置は、前記乱数の所定ビット長と等しいブロック長を有する転置情報を前記受信装置の公開鍵により暗号化した暗号化転置情報を生成し、
通信メッセージの先頭ビットから前記乱数の所定ビット長に等しい長さの各ビットにより構成された第 1 の領域の通信メッセージに対しては、前記転置情報に基づいて、これらの各ビットを前記乱数の所定ビット長と等しいブロック長の転置を施した転置メッセージの各ビットと、前記乱数の先頭ビットから所定ビット長までの各ビットと、をそれぞれ互いに排他的論理和演算することにより、第 1 の暗号化メッセージを生成し、
前記乱数の所定ビット長を超える前記通信メッセージの各ビットから構成された第 2 の領域の通信メッセージに対しては、前記転置情報に基づいて、これらの各ビットを前記転置のブロック長の単位毎に転置を施した転置メッセージの各ビットと、前記通信メッセージの該ビット位置から前記乱数の所定ビット長を減じたビット位置の前記通信メッセージの各ビットと、をそれぞれ互いに排他的論理和演算することにより、第 2 の暗号化メッセージを生成し、
前記暗号化転置情報と第 1 の暗号化メッセージと第 2 の暗号化メッセージとを接続して前記送信装置から前記受信装置へ通信し、
前記受信装置は、
自らの秘密鍵により前記暗号化転置情報から転置情報を復号化し、
第 1 の暗号化メッセージに対しては、これらの各ビットと、前記乱数の先頭ビットから所定ビット長までの各ビットと、をそれぞれ互いに排他的論理和演算して得られた転置メッセージに前記転置の逆写像の転置を施して第 1 の領域の通信メッセージを復号化し、
第 2 の暗号化メッセージに対しては、これらの各ビットと、該ビット位置から前記乱数の所定ビット長を減じたビット位置の前記通信メッセージの各ビットと、をそれぞれ互いに排他的論理和演算して得られた転置メッセージに前記転置の逆写像の転置を施して第 2 の領域の通信メッセージを復号化することを特徴とするストリーム暗号による通信方法。

7

より、第1の暗号化メッセージを生成し、
 前記乱数の所定ビット長を超える前記通信メッセージの各ビットから構成された第2の領域の通信メッセージに対しては、前記転置情報に基づいて、これらの各ビットを前記転置のブロック長の単位毎に転置を施した転置メッセージの各ビットと、前記通信メッセージの該ビット位置から前記乱数の所定ビット長を減じたビット位置の前記通信メッセージの各ビットと、をそれぞれ互いに排他的論理和演算することにより、第2の暗号化メッセージを生成し、
 前記暗号化転置情報と第1の暗号化メッセージと第2の暗号化メッセージとを接続して前記送信装置から前記受信装置へ通信し、
 前記受信装置は、
 自らの秘密鍵により前記暗号化転置情報から転置情報を復号化し、
 第1の暗号化メッセージに対しては、これらの各ビットと、前記乱数の先頭ビットから所定ビット長までの各ビットと、をそれぞれ互いに排他的論理和演算して得られた転置メッセージに前記転置の逆写像の転置を施して第1の領域の通信メッセージを復号化し、
 第2の暗号化メッセージに対しては、これらの各ビットと、該ビット位置から前記乱数の所定ビット長を減じたビット位置の前記通信メッセージの各ビットと、をそれぞれ互いに排他的論理和演算して得られた転置メッセージに前記転置の逆写像の転置を施して第2の領域の通信メッセージを復号化することを特徴とするストリーム暗号による通信方法。
 【請求項13】公開鍵暗号により暗号化した乱数と、公開鍵暗号により暗号化した転置情報と、ストリーム暗号化した通信メッセージと、を送信装置から受信装置へ送るストリーム暗号による通信方法であって、
 前記送信装置は、
 所定のビット長を有する乱数を発生させ、該乱数を受信装置の公開鍵により暗号化して、暗号化乱数を生成し、前記乱数の所定ビット長と等しいブロック長を有する転置情報を前記受信装置の公開鍵により暗号化した暗号化転置情報を生成し、
 通信メッセージの先頭ビットから前記乱数の所定ビット長に等しい長さの各ビットにより構成された第1の領域の通信メッセージに対しては、前記転置情報に基づいて、これらの各ビットを前記乱数の所定ビット長と等しいブロック長の転置を施した転置メッセージの各ビットと、前記乱数の先頭ビットから所定ビット長までの各ビットと、をそれぞれ互いに排他的論理和演算することにより、第1の暗号化メッセージを生成し、
 前記乱数の所定ビット長を超える前記通信メッセージの各ビットから構成された第2の領域の通信メッセージに対しては、前記転置情報に基づいて、これらの各ビットを前記転置のブロック長の単位毎に転置を施した転置メ

(5)

特開平10-84339

8

ッセージの各ビットと、前記通信メッセージの該ビット位置から前記乱数の所定ビット長を減じたビット位置の前記通信メッセージの各ビットと、をそれぞれ互いに排他的論理和演算することにより、第2の暗号化メッセージを生成し、
 前記暗号化乱数と前記暗号化転置情報と第1及び第2の暗号化メッセージとを接続して、送信装置から受信装置へ通信し、
 前記受信装置は、
 10 自らの秘密鍵により、前記暗号化乱数及び前記暗号化転置情報からそれぞれ前記乱数及び前記転置情報を復号化し、
 第1の暗号化メッセージに対しては、これらの各ビットと、前記乱数の先頭ビットから所定ビット長までの各ビットと、をそれぞれ互いに排他的論理和演算して得られた転置メッセージに前記転置の逆写像の転置を施して第1の領域の通信メッセージを復号化し、
 第2の暗号化メッセージに対しては、これらの各ビットと、該ビット位置から前記乱数の所定ビット長を減じたビット位置の前記通信メッセージの各ビットと、をそれぞれ互いに排他的論理和演算して得られた転置メッセージに前記転置の逆写像の転置を施して第2の領域の通信メッセージを復号化することを特徴とするストリーム暗号による通信方法。
 【請求項14】前記乱数のビット数は、前記公開鍵暗号により1度に暗号化可能なビット長を超えるビット数であり、前記乱数が複数の部分に分割されてそれぞれ暗号化され、復号化後に1つの乱数として接続されて暗号化メッセージの復号化に利用されることを特徴とする請求項12または請求項13に記載のストリーム暗号による通信方法。
 【請求項15】それぞれ乱数発生器を備えた送信装置と受信装置との間で、公開鍵暗号を用いる暗号化通信により、乱数発生アルゴリズム及びまたは乱数の初期値を共有することにより、双方の乱数発生器から所定ビット長の同一の乱数を発生させ、
 前記送信装置は、前記乱数の所定ビット長と等しいブロック長を有する転置情報を前記受信装置の公開鍵により暗号化した暗号化転置情報を生成し、
 40 通信メッセージの先頭ビットから前記乱数の所定ビット長に等しい長さの各ビットにより構成された第1の領域の通信メッセージに対しては、前記転置情報に基づいて、これらの各ビットを前記乱数の所定ビット長と等しいブロック長の転置を施した転置メッセージの各ビットと、前記乱数の先頭ビットから所定ビット長までの各ビットと、をそれぞれ互いに排他的論理和演算することにより、第1の暗号化メッセージを生成し、
 前記乱数の所定ビット長を超える前記通信メッセージの各ビットから構成された第2の領域の通信メッセージに対しては、前記転置情報に基づいて、これらの各ビット

50

9

を前記転置のブロック長の単位毎に転置を施した転置メッセージの各ビットと、前記通信メッセージの該ビット位置から前記乱数の所定ビット長を減じたビット位置の前記通信メッセージの各ビットと、をそれぞれ互いに排他的論理和演算することにより、第2の暗号化メッセージを生成し、

前記暗号化転置情報と第1の暗号化メッセージと第2の暗号化メッセージとを接続して前記送信装置から前記受信装置へ通信し、

前記受信装置は、

自らの秘密鍵により前記暗号化転置情報から転置情報を復号化し、

第1の暗号化メッセージに対しては、これらの各ビットと、前記乱数の先頭ビットから所定ビット長までの各ビットと、をそれぞれ互いに排他的論理和演算して得られた転置メッセージに前記転置の逆写像の転置を施して第1の領域の通信メッセージを復号化し、

第2の暗号化メッセージに対しては、これらの各ビットと、該ビット位置から前記乱数の所定ビット長を減じたビット位置の前記通信メッセージの各ビットと、をそれぞれ互いに排他的論理和演算して得られた転置メッセージに前記転置の逆写像の転置を施して第2の領域の通信メッセージを復号化することを特徴とするストリーム暗号による通信方法。

【請求項16】前記送信装置及び受信装置にそれぞれ備えられた乱数発生器から、発生される乱数の周期を超えて、それぞれ乱数を取り出すことを特徴とする請求項15に記載のストリーム暗号による通信方法。

【請求項17】通信メッセージの先頭から所定のビット長を第1の領域の通信メッセージとし、前記通信メッセージの所定のビット長を超える部分を第2の領域の通信メッセージとする通信メッセージの分割を行い、

第1の領域の通信メッセージに対しては公開鍵暗号により、第2の領域の通信メッセージに対してはストリーム暗号により、それぞれ送信装置から受信装置へ通信する通信方法であって、

前記送信装置は、

前記乱数の所定ビット長と等しいブロック長を有する転置情報を前記受信装置の公開鍵により暗号化した暗号化転置情報を生成し、

第1の領域の通信メッセージを前記転置情報に基づいて転置した第1の転置メッセージを前記受信装置の公開鍵により暗号化して、第1の暗号化メッセージを生成し、第2の領域の通信メッセージに該当する前記分割前の通信メッセージの各ビットに対しては、前記転置情報に基づいて、これらの通信メッセージを構成する各ビットを前記転置のブロック長の単位毎に転置を施した第2の転置メッセージの各ビットと、前記通信メッセージの該ビット位置から前記乱数の所定ビット長を減じたビット位置の第1の通信メッセージの各ビットと、をそれぞれ互

(6)

特開平10-84339

10

いに排他的論理和演算することにより、第2の暗号化メッセージを生成し、

前記暗号化転置情報と第1の暗号化メッセージと第2の暗号化メッセージとを接続して送信し、

前記受信装置は、

自らの秘密鍵により、前記暗号化転置情報及び第1の暗号化メッセージからそれぞれ前記転置情報及び第1の転置メッセージを復号化し、この第1の転置メッセージに前記転置の逆写像の転置を施して第1の領域の通信メッセージを復号化し、

第2の暗号化メッセージの各ビットに対しては、これらの各ビットと、該ビット位置が対応する通信メッセージのビット位置から前記所定のビット長を減じたビット位置の復号化された通信メッセージの各ビットと、をそれぞれ互いに排他的論理和演算することにより、第2の領域の通信メッセージを復号化することを特徴とするストリーム暗号による通信方法。

【請求項18】前記第1の領域の通信メッセージのビット数は、前記公開鍵暗号により1度に暗号化可能なビット数を超えるビット数であり、それぞれ複数回の暗号化及び復号化によって第1の領域の通信メッセージの暗号化及び復号化が行われることを特徴とする請求項17に記載のストリーム暗号による通信方法。

【請求項19】前記排他的論理和演算を行う処理を、複数ビット並列して実行させることを特徴とする請求項1ないし請求項18のいずれか1項に記載のストリーム暗号による通信方法。

【請求項20】前記第2の領域の通信メッセージを暗号化または復号化するための排他的論理和演算の処理は、少なくとも一方の演算対象データを前記第1の領域の通信メッセージのビット数だけシフトする動作を含むことを特徴とする請求項1ないし請求項19のいずれか1項に記載の、ストリーム暗号による通信方法。

【請求項21】送信装置と受信装置との間で所定のビット長の乱数を共有させる乱数共有化手段と、

通信メッセージの先頭ビットから前記乱数の所定ビット長に等しい長さの各ビットに対しては、前記乱数の先頭ビットから所定ビット長までの各ビットと排他的論理和演算し、前記乱数の所定ビット長を超える前記通信メッセージの各ビットに対しては、該ビット位置から前記乱数の所定ビット長を減じたビット位置の前記通信メッセージの各ビットと排他的論理和演算することにより暗号化メッセージを生成する暗号化手段を備えた送信装置と、

前記暗号化メッセージの先頭ビットから前記乱数の所定ビット長に等しい長さの各ビットに対しては、前記乱数の先頭ビットから所定ビット長までの各ビットと排他的論理和演算し、前記乱数の所定ビット長を超える前記暗号化メッセージの各ビットに対しては、該ビット位置から前記乱数の所定ビット長を減じたビット位置の前記暗

11

号化メッセージの各ビットと排他的論理和演算することにより復号化メッセージを得る復号化手段を備えた受信装置と、
を備えたことを特徴とするストリーム暗号による通信システム。

【請求項 2 2】前記乱数共有化手段は、
前記送信装置と前記受信装置との間で、それぞれ個別に生成された異なる乱数に基づいて生成された情報を互いに交換し、この交換された情報及び前記個別に生成された異なる乱数に基づいて、前記送信装置及び前記受信装置がそれぞれ同一の共有乱数を生成するものであることを特徴とする請求項 2 1 に記載のストリーム暗号による通信システム。

【請求項 2 3】前記乱数共有化手段は、
前記受信装置の公開鍵により公開鍵暗号化された乱数を送信装置より送信する公開鍵暗号化手段と、
この公開鍵暗号化された乱数を受信し受信装置自身の秘密鍵により乱数を復号化する公開鍵復号化手段と、
を備えたものであることを特徴とする請求項 2 1 に記載のストリーム暗号による通信システム。

【請求項 2 4】前記乱数共有化手段は、
前記送信装置に設けられた乱数発生アルゴリズム及びまたは乱数の初期値を設定可能な第 1 の乱数発生器と、
前記乱数発生アルゴリズム及びまたは乱数の初期値を前記受信装置の公開鍵により公開鍵暗号化する公開鍵暗号化手段と、
この公開鍵暗号化された乱数発生アルゴリズム及びまたは乱数の初期値を受信装置自身の秘密鍵により復号化する公開鍵復号化手段と、
前記受信装置に設けられ、この復号化された乱数発生アルゴリズム及びまたは乱数の初期値を設定可能な第 2 の乱数発生器と、
を備えたことを特徴とする請求項 2 1 に記載のストリーム暗号による通信システム。

【請求項 2 5】それぞれ乱数の初期値を構成するビットの値が外部より設定される複数ビットのシフトレジスタと、
このシフトレジスタの各ビットから新たな乱数を生成するためのビットを指定するための値が乱数発生アルゴリズムとして外部より設定される制御レジスタと、
前記制御レジスタの値により指定されたシフトレジスタのビット間で排他的論理和演算を行い、その結果をシフトレジスタに入力する排他的論理和回路と、
を備えた乱数発生器を送信装置及び受信装置がそれぞれ備えてなり、
両装置の乱数発生器が互いに等しい乱数を生成することを特徴とするストリーム暗号による通信システム。

【請求項 2 6】前記送信装置は、
転置情報に基づいて、前記乱数の所定ビット長に等しいブロック長を有するブロック単位に前記通信メッセージ

(7)

特開平 1 0 - 8 4 3 3 9

12

のビット位置を入れ替える第 1 の転置手段と、
前記転置情報を受信装置の公開鍵により暗号化し暗号化転置情報を生成する公開鍵暗号化手段と、をさらに備えてなり、

前記受信装置は、
自身の秘密鍵により前記暗号化転置情報を復号化し転置情報を生成する公開鍵復号化手段と、

この復号化された転置情報に基づいて、該転置情報の示す転置の逆写像を前記復号化メッセージに施す第 2 の転置手段と、

を備えたことを特徴とする請求項 2 1 に記載のストリーム暗号による通信システム。

【請求項 2 7】前記暗号化手段または前記復号化手段は、

共有乱数が初期状態として設定されるとともにシフトイン入力に通信メッセージまたは暗号化メッセージの直列供給源が接続されたシフトレジスタと、

このシフトレジスタのシフトアウト出力に一方の入力が接続され、前記通信メッセージまたは暗号化メッセージの直列供給源に他方の入力が接続され、その出力が暗号化メッセージまたは復号化された通信メッセージとなる 2 入力排他的論理和回路と、

を備えたことを特徴とする請求項 2 1 に記載のストリーム暗号による通信システム。

【請求項 2 8】前記シフトレジスタまたは該シフトレジスタ及び前記排他的論理和回路を備えた回路が単一の集積回路に集積化されたことを特徴とする請求項 2 7 に記載のストリーム暗号による通信システム。

【請求項 2 9】前記暗号化手段及びまたは前記復号化手段は、

前記排他的論理和演算を複数ビット並列に行う演算器を備えたことを特徴とする請求項 2 1 に記載のストリーム暗号による通信システム。

【請求項 3 0】所定のビット幅で順次供給される第 1 のデータを一時保持する第 1 の保持手段と、前記所定のビット幅の第 2 のデータまたは第 1 の保持手段に保持されたデータを一時保持する第 2 の保持手段と、第 1 及び第 2 の保持手段の内容をそれぞれビット毎に排他的論理和演算を行う前記所定ビット幅の並列演算器と、を備えた回路を単一の集積回路に集積化したことを特徴とするストリーム暗号による通信システム。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】本発明は、ストリーム暗号による通信方法、ならびに通信システムに係り、特に秘密鍵の共有のための処理時間を短縮することにより高速化を図ったストリーム暗号による通信方法、ならびに通信システムに関する。

【0 0 0 2】

【従来の技術】暗号方式は、秘密鍵暗号と公開鍵暗号に

50

大きく分類できる。秘密鍵暗号は、通信相手同士が共有した秘密鍵を用いて暗号化及び復号化を行うもので、一般に公開鍵暗号に比べて暗号化・復号化を高速に行えるが、鍵の配送という問題がある。公開鍵暗号は、鍵の配送の問題を解決するが、暗号化及び復号化の処理量が多く、リアルタイム性のあるマルチメディア情報の秘密通信への利用には困難がある。また、秘密鍵暗号は、公開鍵暗号に比べて処理が高速であるとはいえ、やはりリアルタイム情報の秘密通信への利用にはさらに高速な暗号方式が望まれる。

【0003】理論的に最も安全で、しかも暗号化・復号化の処理量の少ない秘密鍵暗号としては、一回限りの使い捨て鍵（ワンタイム・パッド、以下単にパッドとも略

$$c_i = m_i + k_i \pmod{2} \quad (i = 1, 2, \dots) \quad \dots (1)$$

式(1)となる。 $\text{mod } 2$ での和は、いわゆる排他的論理和であり、以下、 $(+)$ で排他的論理和を表すとすれば、式(1)の暗号化は、

$$\text{【数2】 } c_i = m_i (+) k_i \quad \dots (2)$$

$$m_i = c_i (+) k_i = m_i (+) k_i (+) k_i = m_i \quad \dots (3)$$

式(3)と表される。ここで、 k_i の値が0, 1にかかわらず、 $k_i (+) k_i \equiv 0$ が成立する。

【0007】しかしながら、このようなパーナム暗号を利用するためには、あらかじめ通信データ量と同じ量の秘密鍵を共有しておく必要がある。

【0008】秘密鍵の共有方法として、従来より公開鍵配送法が知られている。公開鍵配送法は、通信相手同士がそれぞれ秘密鍵を作成し、公開鍵を利用してそれぞれの秘密鍵にある演算を施して得た情報（これは盗聴されてもかまわない）を交換し、それぞれの秘密鍵とこの交換した情報とに基づいて、共有の秘密鍵を生成するものである。

【0009】次に、従来の公開鍵配送法の例として、デ

$$Y_A = \alpha^{X_A} \pmod{p}, \quad 1 \leq Y_A \leq p-1 \quad \dots (4)$$

を計算し、 Y_A をBに送る。Bは、

$$Y_B = \alpha^{X_B} \pmod{p}, \quad 1 \leq Y_B \leq p-1 \quad \dots (5)$$

を計算し、 Y_B をAに送る。

【0012】このように Y_A , Y_B を交換してから、Aは共有鍵 K を次のように計算する。

$$\begin{aligned} K &= (Y_B)^{X_A} \pmod{p} \\ &= (\alpha^{X_B} \pmod{p})^{X_A} \pmod{p} \\ &= \alpha^{X_B X_A} \pmod{p}, \quad 1 \leq K \leq p-1 \quad \dots (6) \end{aligned}$$

Bも同様にして、共有鍵 K を次のように計算する。

【数7】

【0014】

$$\begin{aligned} K &= (Y_A)^{X_B} \pmod{p} \\ &= (\alpha^{X_A} \pmod{p})^{X_B} \pmod{p} \\ &= \alpha^{X_A X_B} \pmod{p}, \quad 1 \leq K \leq p-1 \quad \dots (7) \end{aligned}$$

以上の方法でAとBは、鍵 $K = \alpha^{X_A X_B} \pmod{p}$ を秘密に共有できる。このDH型公開鍵配送法の構成を図27に示す。

【0015】ここで、第3者が Y_A と Y_B とを盗聴して

す)を使用し、通信データとパッドとをビット毎に排他的論理和演算を行なうパーナム暗号が知られている。

【0004】パーナム暗号は、図26に示すように、平文と同じ長さの2進乱数列（以下、単に乱数と呼ぶ）を秘密鍵として用い、平文のビット列と乱数のビット列とを1ビットずつ排他的論理和演算して暗号文のビット列を生成し、同じ秘密鍵を用いて復号化するストリーム暗号（逐次暗号とも呼ばれる）の一種である。

【0005】ここで、平文のビット列を $M = m_1, m_2, \dots$ とし、鍵のビット列を $K = k_1, k_2, \dots$ とすると、暗号文のビット列 $C = c_1, c_2, \dots$ は、

【数1】

式(2)と表される。

【0006】復号化は同じ鍵を用いて、

【数3】

ィフィ・ヘルマン（Diffie-Hellman）型公開鍵配送法

（以下、DH型公開鍵配送法と略す）を説明する（参考文献「現代暗号理論」電子通信学会発行）。

【0010】利用者Aと利用者Bとの間でDH型公開鍵配送法を適用するとする。素数 p とガロア体 $GF(p)$ のある固定された原始根 α の値は、公開鍵として事前に知らせておく。まず、Aは区間 $[0, p-1]$ の間の整数 X_A をランダムに選び、秘密に保持しておく。Bも同様に区間 $[0, p-1]$ の間の整数 X_B をランダムに選び、秘密に保持しておく。

【0011】そして、Aは、

【数4】

【数5】

【0013】

【数6】

も、 X_A と X_B と K を推定することはできない。なお、 Y_A と Y_B の積 Z は、 $Z = \alpha^{(X_A + X_B)} \pmod{p}$ であり、 K とは異なることに留意されたい。もちろん、素数 p と原始根 α の値や Z の値が分かっても推定できないこ

とに変わりはなく、秘密鍵Kを知ろうとする第3者は、

$$K = (YA) (\text{LOG}_\alpha YB) \bmod p$$

$$K = (YB) (\text{LOG}_\alpha YA) \bmod p$$

式(8)または(9)を計算しなければならず、これはいわゆる離散対数を解く計算量が必要である。

【0016】このDH型公開鍵配送法では、共有鍵を変更するのに公開鍵を書き換える必要がある。ところが公開ファイルの鍵リストを変更するには、公開ファイル进行管理している鍵センターとの通信、本人であることの認証など様々な手間がかかるので、DH型公開鍵配送法の基本方式では頻繁に鍵を変更することは出来ない。

【0017】そこで、本人が登録したことを認証した公開鍵をもとに、様々な値の共有鍵を生成する方法、すなわち、公開鍵を変更せずに、共有の暗号鍵を変更する拡張DH型公開鍵配送方式が提案されている(山元、秋山「A data encryption device incorporating fast PKD S」Global Com. 32. 2. 1-32. 2. 6(Dec. 1983)、岡本、中村「公開鍵配送方式の一検討」昭和59年電子情報通信学会全国大会15、松本、高嶋、今井、「公開鍵配送方式に関する二三の考察」CIS研資 1985-02)。

【0018】また、秘密鍵の共有のために、RSA暗号等の公開鍵暗号による秘密鍵の配送も行われているが、公開鍵暗号のブロックサイズにより秘密鍵の長さが限定され、かつ、暗号化及び復号化のための処理量が多く、秘密鍵共有のための処理時間が多くかかっていた。

【0019】また、ブロック単位の暗号化を行う秘密鍵暗号としてDES暗号等が知られている。DES暗号は、比較的短い56ビットの秘密鍵を利用して転置と換字を繰り返し、64ビットの平文ブロックと64ビットの暗号文ブロックとを相互に変換するものである。

【0020】

【発明が解決しようとする課題】以上説明したように、上記従来のバーナム暗号等のストリーム暗号においては、通信相手同士で予めメッセージ長と同じ長さの乱数列である秘密鍵を共有しておく必要があり、この秘密鍵を安全に配送しなければならないという問題点があった。

【0021】また、この秘密鍵の共有に公開鍵配送法や公開鍵暗号を使うと、公開鍵暗号による暗号化及び復号化の処理量が膨大となり、秘密鍵を使用するストリーム暗号本来の高速性が失われるという問題点があった。

【0022】また、DES暗号等のブロック秘密鍵暗号では、共有すべき秘密鍵は比較的短い、高価な専用ハードウェアを用意しなければならないという問題点があった。

【0023】以上の問題点に鑑み、本発明の主要な課題は、従来の秘密鍵暗号の鍵配送問題を解決し、少量の秘密鍵の配送だけで、大量の通信メッセージの秘密鍵暗号による通信を可能とすることである。

【0024】また本発明の別の課題は、従来の秘密鍵暗

【数8】

$$\dots (8)$$

$$\dots (9)$$

号あるいは公開鍵暗号と同等の安全性を確保した暗号通信を行うことである。

【0025】また本発明の別の課題は、リアルタイム性のあるマルチメディア情報の秘密通信に適用可能とするため、従来型の秘密鍵暗号や公開鍵暗号と比べて、暗号化および復号化の処理量が少なく、リアルタイムの暗号化及び復号化が行えるストリーム暗号による通信方法及び通信システムを提供することである。

【0026】さらに本発明の別の課題は、暗号化及び復号化の処理をさらに高速化するために、並列処理が可能であり、またハードウェア化が容易であるストリーム暗号による通信方法及び通信システムを提供することである。

【0027】

【課題を解決するための手段】上記課題を解決するため、本発明は次の構成を有する。すなわち、請求項1記載の発明は、送信装置と受信装置との間で、予め所定ビット長を有する乱数を共有し、前記送信装置は、通信メッセージの先頭ビットから前記乱数の所定ビット長に等しい長さの各ビットにより構成された第1の領域の通信メッセージに対しては、これらの各ビットと、前記乱数の先頭ビットから所定ビット長までの各ビットと、をそれぞれ互いに排他的論理和演算することにより、第1の暗号化メッセージを生成し、前記乱数の所定ビット長を超える前記通信メッセージの各ビットから構成された第2の領域の通信メッセージに対しては、これらの各ビットと、該ビット位置から前記乱数の所定ビット長を減じたビット位置の前記通信メッセージの各ビットと、をそれぞれ互いに排他的論理和演算することにより、第2の暗号化メッセージを生成し、第1及び第2の暗号化メッセージを前記送信装置から前記受信装置へ通信し、前記受信装置は、第1の暗号化メッセージに対しては、これらの各ビットと、前記乱数の先頭ビットから所定ビット長までの各ビットと、をそれぞれ互いに排他的論理和演算することにより、第1の暗号化メッセージから第1の領域の通信メッセージを復号化し、第2の暗号化メッセージに対しては、これらの各ビットと、該ビット位置から前記乱数の所定ビット長を減じたビット位置の前記通信メッセージの各ビットと、をそれぞれ互いに排他的論理和演算することにより、第2の暗号化メッセージから第2の領域の通信メッセージを復号化する、ことを要旨とするストリーム暗号による通信方法である。

【0028】請求項1に記載の発明によれば、通信メッセージの長さよりも短い秘密鍵である乱数を予め送信装置と受信装置間で共有する。次いで、通信メッセージの先頭からこの乱数のビット長に等しい長さの第1の領域の通信メッセージに対してのみこの乱数の各ビットと排

他の論理和演算し、残りの第2の領域の通信メッセージに対しては、該ビット位置からこの乱数のビット長を減じたビット位置の通信メッセージの各ビットをそれぞれ互いに排他的論理和演算することにより、暗号化メッセージを生成するので、予め共有すべき乱数のビット長を通信メッセージより短縮し、乱数の共有の為の時間を削減し、高速な暗号化通信を行うことができる。

【0029】また、請求項2記載の発明は、送信装置と受信装置との間で、公開鍵配送法により、予め所定ビット長を有する乱数を共有し、前記送信装置は、通信メッセージの先頭ビットから前記乱数の所定ビット長に等しい長さの各ビットにより構成された第1の領域の通信メッセージに対しては、これらの各ビットと、前記乱数の先頭ビットから所定ビット長までの各ビットと、をそれぞれ互いに排他的論理和演算することにより、第1の暗号化メッセージを生成し、前記乱数の所定ビット長を超える前記通信メッセージの各ビットから構成された第2の領域の通信メッセージに対しては、これらの各ビットと、該ビット位置から前記乱数の所定ビット長を減じたビット位置の前記通信メッセージの各ビットと、をそれぞれ互いに排他的論理和演算することにより、第2の暗号化メッセージを生成し、第1及び第2の暗号化メッセージを前記送信装置から前記受信装置へ通信し、前記受信装置は、第1の暗号化メッセージに対しては、これらの各ビットと、前記乱数の先頭ビットから所定ビット長までの各ビットと、をそれぞれ互いに排他的論理和演算することにより、第1の暗号化メッセージから第1の領域の通信メッセージを復号化し、第2の暗号化メッセージに対しては、これらの各ビットと、該ビット位置から前記乱数の所定ビット長を減じたビット位置の前記通信メッセージの各ビットと、をそれぞれ互いに排他的論理和演算することにより、第2の暗号化メッセージから第2の領域の通信メッセージを復号化する、ことを要旨とするストリーム暗号による通信方法である。

【0030】請求項2に記載の発明によれば、通信メッセージの長さよりも短い秘密鍵である乱数を予め公開鍵配送法により送信装置と受信装置間で共有する。公開鍵配送法により秘密鍵である共有乱数の配送の安全性が確保される。次いで、通信メッセージの先頭からこの乱数のビット長に等しい長さの第1の領域の通信メッセージに対してのみこの乱数の各ビットと排他的論理和演算し、残りの第2の領域の通信メッセージに対しては、該ビット位置から前記乱数の所定ビット長を減じたビット位置の前記通信メッセージの各ビットとをそれぞれ互いに排他的論理和演算することにより、暗号化メッセージを生成する。これにより予め共有すべき乱数のビット長を通信メッセージより短縮し、乱数の共有の為の時間を削減し、高速な暗号化通信を行うことができる。

【0031】また、請求項3記載の発明は、送信装置と受信装置との間で、公開鍵暗号による暗号化通信によ

り、予め所定ビット長を有する乱数を共有し、前記送信装置は、通信メッセージの先頭ビットから前記乱数の所定ビット長に等しい長さの各ビットにより構成された第1の領域の通信メッセージに対しては、これらの各ビットと、前記乱数の先頭ビットから所定ビット長までの各ビットと、をそれぞれ互いに排他的論理和演算することにより、第1の暗号化メッセージを生成し、前記乱数の所定ビット長を超える前記通信メッセージの各ビットから構成された第2の領域の通信メッセージに対しては、これらの各ビットと、該ビット位置から前記乱数の所定ビット長を減じたビット位置の前記通信メッセージの各ビットと、をそれぞれ互いに排他的論理和演算することにより、第2の暗号化メッセージを生成し、第1及び第2の暗号化メッセージを前記送信装置から前記受信装置へ通信し、前記受信装置は、第1の暗号化メッセージに対しては、これらの各ビットと、前記乱数の先頭ビットから所定ビット長までの各ビットと、をそれぞれ互いに排他的論理和演算することにより、第1の暗号化メッセージから第1の領域の通信メッセージを復号化し、第2の暗号化メッセージに対しては、これらの各ビットと、該ビット位置から前記乱数の所定ビット長を減じたビット位置の前記通信メッセージの各ビットと、をそれぞれ互いに排他的論理和演算することにより、第2の暗号化メッセージから第2の領域の通信メッセージを復号化する、ことを要旨とするストリーム暗号による通信方法である。

【0032】請求項3に記載の発明によれば、通信メッセージの長さよりも短い秘密鍵である乱数を予め公開鍵暗号方式の通信により送信装置と受信装置との間で共有する。公開鍵暗号により秘密鍵である共有乱数の配送の安全性が確保される。次いで、通信メッセージの先頭からこの乱数のビット長に等しい長さの第1の領域の通信メッセージに対してのみこの乱数の各ビットと排他的論理和演算し、残りの第2の領域の通信メッセージに対しては、該ビット位置から前記乱数の所定ビット長を減じたビット位置の前記通信メッセージの各ビットとをそれぞれ互いに排他的論理和演算することにより、暗号化メッセージを生成する。これにより予め共有すべき乱数のビット長を通信メッセージより短縮し、乱数の共有の為の時間を削減し、高速な暗号化通信を行うことができる。

【0033】また、請求項4記載の発明は、送信装置から受信装置へ、公開鍵暗号により暗号化した乱数と、ストリーム暗号化した通信メッセージと、を送るストリーム暗号による通信方法であって、前記送信装置は、所定ビット長を有する乱数を発生させ、該乱数を受信装置の公開鍵により暗号化して、暗号化乱数を生成し、通信メッセージの先頭ビットから前記乱数の所定ビット長に等しい長さの各ビットにより構成された第1の領域の通信メッセージに対しては、これらの各ビットと、前記乱数

の先頭ビットから所定ビット長までの各ビットと、をそれぞれ互いに排他的論理和演算することにより、第1の暗号化メッセージを生成し、前記乱数の所定ビット長を超える前記通信メッセージの各ビットから構成された第2の領域の通信メッセージに対しては、これらの各ビットと、該ビット位置から前記乱数の所定ビット長を減じたビット位置の前記通信メッセージの各ビットと、をそれぞれ互いに排他的論理和演算することにより、第2の暗号化メッセージを生成し、前記暗号化乱数と第1および第2の暗号化メッセージとを接続して前記送信装置から前記受信装置へ通信し、前記受信装置は、前記暗号化乱数を自らの秘密鍵により復号化して乱数を生成し、第1の暗号化メッセージに対しては、これらの各ビットと、前記乱数の先頭ビットから所定ビット長までの各ビットと、をそれぞれ互いに排他的論理和演算することにより、第1の暗号化メッセージから第1の領域の通信メッセージを復号化し、第2の暗号化メッセージに対しては、これらの各ビットと、該ビット位置から前記乱数の所定ビット長を減じたビット位置の前記通信メッセージの各ビットと、をそれぞれ互いに排他的論理和演算することにより、第2の暗号化メッセージから第2の領域の通信メッセージを復号化する、ことを要旨とするストリーム暗号による通信方法である。

【0034】請求項4に記載の発明によれば、通信メッセージの長さよりも短い秘密鍵である乱数を公開鍵暗号方式により暗号化し、次いで、通信メッセージの先頭からこの乱数のビット長に等しい長さの第1の領域の通信メッセージに対してのみこの乱数の各ビットと排他的論理和演算し、残りの第2の領域の通信メッセージに対しては、該ビット位置から前記乱数の所定ビット長を減じたビット位置の前記通信メッセージの各ビットとをそれぞれ互いに排他的論理和演算することにより、暗号化メッセージを生成する。これにより、公開鍵暗号の持つ安全性により秘密鍵である共有乱数の配送の安全性が確保される。また、共有すべき乱数のビット長を通信メッセージより短縮し、乱数の共有の為に時間を削減し、高速な暗号化通信を行うことができる。

【0035】また請求項5記載の発明は、請求項3または請求項4に記載のストリーム暗号による通信方法において、前記乱数のビット数は、前記公開鍵暗号により1度に暗号化可能なビット数を超えるビット数であり、それぞれ複数回の暗号化及び復号化によって前記乱数の暗号化及び復号化が行われることを要旨とする。

【0036】請求項5記載の発明によれば、公開鍵暗号による暗号化ブロックサイズより大きいビット長の乱数を分割して送ることができるので、公開鍵暗号の制約に拘わらず十分長い乱数を送ることができ、より一層安全性を向上させることができる。

【0037】また、請求項6記載の発明は、それぞれ乱数発生器を備えた送信装置と受信装置との間で、公開鍵

暗号を用いる暗号化通信により、乱数発生アルゴリズム及びまたは乱数の初期値を共有することにより、双方の乱数発生器から所定ビット長の同一の乱数を発生させ、前記送信装置は、通信メッセージの先頭ビットから前記乱数の所定ビット長に等しい長さの各ビットにより構成された第1の領域の通信メッセージに対しては、これらの各ビットと、前記乱数の先頭ビットから所定ビット長までの各ビットと、をそれぞれ互いに排他的論理和演算することにより、第1の暗号化メッセージを生成し、前記乱数の所定ビット長を超える前記通信メッセージの各ビットから構成された第2の領域の通信メッセージに対しては、これらの各ビットと、該ビット位置から前記乱数の所定ビット長を減じたビット位置の前記通信メッセージの各ビットと、をそれぞれ互いに排他的論理和演算することにより、第2の暗号化メッセージを生成し、第1及び第2の暗号化メッセージを前記送信装置から前記受信装置へ通信し、前記受信装置は、第1の暗号化メッセージに対しては、これらの各ビットと、前記乱数の先頭ビットから所定ビット長までの各ビットと、をそれぞれ互いに排他的論理和演算することにより、第1の暗号化メッセージから第1の領域の通信メッセージを復号化し、第2の暗号化メッセージに対しては、これらの各ビットと、該ビット位置から前記乱数の所定ビット長を減じたビット位置の前記通信メッセージの各ビットと、をそれぞれ互いに排他的論理和演算することにより、第2の暗号化メッセージから第2の領域の通信メッセージを復号化することを要旨とするストリーム暗号による通信方法である。

【0038】請求項6に記載の発明によれば、送信装置および受信装置にそれぞれ乱数発生器を備え、公開鍵暗号を用いて、乱数発生アルゴリズム及びまたは乱数の初期値を送信装置から受信装置へ送ることにより、双方の乱数発生器を互いに等しい状態に設定することができ、双方の乱数発生器から等しい乱数を発生することにより、秘密鍵である乱数を共有することができる。公開鍵暗号により乱数発生アルゴリズム及びまたは乱数の初期値の配送の安全性が確保される。また乱数そのものではなく、乱数発生アルゴリズム及びまたは乱数の初期値を送ることにより、乱数共有のための通信が短縮され、乱数共有の為に時間を削減し、高速な暗号化通信を行うことができる。

【0039】また請求項7記載の発明は、請求項6に記載のストリーム暗号による通信方法において、前記送信装置及び受信装置にそれぞれ備えられた乱数発生器から、発生される乱数の周期を超えて、それぞれ乱数を取り出すことを要旨とする。これにより、十分に長い乱数を利用することができる。

【0040】また、請求項8記載の発明は、通信メッセージの先頭から所定のビット長を第1の領域の通信メッセージとし、前記通信メッセージの所定のビット長を超

える部分を第2の領域の通信メッセージとする通信メッセージの分割を行い、第1の領域の通信メッセージに対しては公開鍵暗号により、第2の領域の通信メッセージに対してはストリーム暗号により、それぞれ送信装置から受信装置へ通信する通信方法であって、前記送信装置は、第1の領域の通信メッセージを受信装置の公開鍵により暗号化して、第1の暗号化メッセージを生成し、第2の領域の通信メッセージに対しては、これらの各ビットと、該ビット位置から前記第1の領域の通信メッセージのビット長を減じたビット位置の前記通信メッセージの各ビットと、をそれぞれ互いに排他的論理和演算することにより、第2の暗号化メッセージを生成し、前記第1および第2の暗号化メッセージを接続して前記送信装置から前記受信装置へ通信し、前記受信装置は、自らの秘密鍵により、前記第1の暗号化メッセージから第1の領域の通信メッセージを復号化し、前記第2の暗号化メッセージの各ビットに対しては、これらの各ビットと、該ビット位置が対応する前記通信メッセージのビット位置から前記所定のビット長を減じたビット位置の復号化された通信メッセージの各ビットと、をそれぞれ互いに排他的論理和演算することにより、第2の暗号化メッセージから第2の領域の通信メッセージを復号化する、ことを要旨とするストリーム暗号による通信方法である。

【0041】請求項8記載の発明によれば、通信メッセージの先頭から所定のビット長までの第1の領域の通信メッセージを公開鍵暗号化し、残りの通信メッセージは、これらの各ビットと、該ビット位置から前記第1の領域の通信メッセージのビット長を減じたビット位置の前記通信メッセージの各ビットと、をそれぞれ互いに排他的論理和演算することによりストリーム暗号化する。公開鍵暗号の持つ安全性により、第1の領域の通信メッセージの安全性が確保され、第2の領域の通信メッセージの復号化は、第1の領域の通信メッセージの復号化が前提となる。これにより、乱数を共有化することなく、高速で安全性の高い暗号化が行える。

【0042】また請求項9記載の発明は、請求項8に記載のストリーム暗号による通信方法において、前記第1の領域の通信メッセージのビット数は、前記公開鍵暗号により1度に暗号化可能なビット数を超えるビット数であり、それぞれ複数回の暗号化及び復号化によって第1の領域の通信メッセージの暗号化及び復号化が行われることを要旨とする。

【0043】請求項9記載の発明によれば、公開鍵暗号化する第1の領域の通信メッセージの長さが利用する公開鍵暗号方式に限定されず、十分な安全性を確保できる長さとすることができる。

【0044】また、請求項10記載の発明は、送信装置と受信装置との間で、予め所定ビット長を有する乱数を共有し、前記送信装置は、前記乱数の所定ビット長と等しいブロック長を有する転置情報を前記受信装置の公開

鍵により暗号化した暗号化転置情報を生成し、通信メッセージの先頭ビットから前記乱数の所定ビット長に等しい長さの各ビットにより構成された第1の領域の通信メッセージに対しては、前記転置情報に基づいて、これらの各ビットを前記乱数の所定ビット長と等しいブロック長の転置を施した転置メッセージの各ビットと、前記乱数の先頭ビットから所定ビット長までの各ビットと、をそれぞれ互いに排他的論理和演算することにより、第1の暗号化メッセージを生成し、前記乱数の所定ビット長を超える前記通信メッセージの各ビットから構成された第2の領域の通信メッセージに対しては、前記転置情報に基づいて、これらの各ビットを前記転置のブロック長の単位毎に転置を施した転置メッセージの各ビットと、前記通信メッセージの該ビット位置から前記乱数の所定ビット長を減じたビット位置の前記通信メッセージの各ビットと、をそれぞれ互いに排他的論理和演算することにより、第2の暗号化メッセージを生成し、前記暗号化転置情報と第1の暗号化メッセージと第2の暗号化メッセージとを接続して前記送信装置から前記受信装置へ通信し、前記受信装置は、自らの秘密鍵により前記暗号化転置情報から転置情報を復号化し、第1の暗号化メッセージに対しては、これらの各ビットと、前記乱数の先頭ビットから所定ビット長までの各ビットと、をそれぞれ互いに排他的論理和演算して得られた転置メッセージに前記転置の逆写像の転置を施して第1の領域の通信メッセージを復号化し、第2の暗号化メッセージに対しては、これらの各ビットと、該ビット位置から前記乱数の所定ビット長を減じたビット位置の前記通信メッセージの各ビットと、をそれぞれ互いに排他的論理和演算して得られた転置メッセージに前記転置の逆写像の転置を施して第2の領域の通信メッセージを復号化する、ことを要旨とするストリーム暗号による通信方法である。

【0045】また、請求項11記載の発明は、送信装置と受信装置との間で、公開鍵配送法により、予め所定ビット長を有する乱数を共有し、前記送信装置は、前記乱数の所定ビット長と等しいブロック長を有する転置情報を前記受信装置の公開鍵により暗号化した暗号化転置情報を生成し、通信メッセージの先頭ビットから前記乱数の所定ビット長に等しい長さの各ビットにより構成された第1の領域の通信メッセージに対しては、前記転置情報に基づいて、これらの各ビットを前記乱数の所定ビット長と等しいブロック長の転置を施した転置メッセージの各ビットと、前記乱数の先頭ビットから所定ビット長までの各ビットと、をそれぞれ互いに排他的論理和演算することにより、第1の暗号化メッセージを生成し、前記乱数の所定ビット長を超える前記通信メッセージの各ビットから構成された第2の領域の通信メッセージに対しては、前記転置情報に基づいて、これらの各ビットを前記転置のブロック長の単位毎に転置を施した転置メッセージの各ビットと、前記通信メッセージの該ビット位

置から前記乱数の所定ビット長を減じたビット位置の前記通信メッセージの各ビットと、をそれぞれ互いに排他的論理和演算することにより、第2の暗号化メッセージを生成し、前記暗号化転置情報と第1の暗号化メッセージと第2の暗号化メッセージとを接続して前記送信装置から前記受信装置へ通信し、前記受信装置は、自らの秘密鍵により前記暗号化転置情報から転置情報を復号化し、第1の暗号化メッセージに対しては、これらの各ビットと、前記乱数の先頭ビットから所定ビット長までの各ビットと、をそれぞれ互いに排他的論理和演算して得られた転置メッセージに前記転置の逆写像の転置を施して第1の領域の通信メッセージを復号化し、第2の暗号化メッセージに対しては、これらの各ビットと、該ビット位置から前記乱数の所定ビット長を減じたビット位置の前記通信メッセージの各ビットと、をそれぞれ互いに排他的論理和演算して得られた転置メッセージに前記転置の逆写像の転置を施して第2の領域の通信メッセージを復号化することを要旨とするストリーム暗号による通信方法である。

【0046】また、請求項12記載の発明は、送信装置と受信装置との間で、公開鍵暗号による暗号化通信により、予め所定ビット長を有する乱数を共有し、前記送信装置は、前記乱数の所定ビット長と等しいブロック長を有する転置情報を前記受信装置の公開鍵により暗号化した暗号化転置情報を生成し、通信メッセージの先頭ビットから前記乱数の所定ビット長に等しい長さの各ビットにより構成された第1の領域の通信メッセージに対しては、前記転置情報に基づいて、これらの各ビットを前記乱数の所定ビット長と等しいブロック長の転置を施した転置メッセージの各ビットと、前記乱数の先頭ビットから所定ビット長までの各ビットと、をそれぞれ互いに排他的論理和演算することにより、第1の暗号化メッセージを生成し、前記乱数の所定ビット長を超える前記通信メッセージの各ビットから構成された第2の領域の通信メッセージに対しては、前記転置情報に基づいて、これらの各ビットを前記転置のブロック長の単位毎に転置を施した転置メッセージの各ビットと、前記通信メッセージの該ビット位置から前記乱数の所定ビット長を減じたビット位置の前記通信メッセージの各ビットと、をそれぞれ互いに排他的論理和演算することにより、第2の暗号化メッセージを生成し、前記暗号化転置情報と第1の暗号化メッセージと第2の暗号化メッセージとを接続して前記送信装置から前記受信装置へ通信し、前記受信装置は、自らの秘密鍵により前記暗号化転置情報から転置情報を復号化し、第1の暗号化メッセージに対しては、これらの各ビットと、前記乱数の先頭ビットから所定ビット長までの各ビットと、をそれぞれ互いに排他的論理和演算して得られた転置メッセージに前記転置の逆写像の転置を施して第1の領域の通信メッセージを復号化し、第2の暗号化メッセージに対しては、これらの各ビ

ットと、該ビット位置から前記乱数の所定ビット長を減じたビット位置の前記通信メッセージの各ビットと、をそれぞれ互いに排他的論理和演算して得られた転置メッセージに前記転置の逆写像の転置を施して第2の領域の通信メッセージを復号化する、ことを要旨とするストリーム暗号による通信方法である。

【0047】また請求項13記載の発明は、公開鍵暗号により暗号化した乱数と、公開鍵暗号により暗号化した転置情報と、ストリーム暗号化した通信メッセージと、を送信装置から受信装置へ送るストリーム暗号による通信方法であって、前記送信装置は、所定ビット長を有する乱数を発生させ、該乱数を受信装置の公開鍵により暗号化して暗号化乱数を生成し、前記乱数の所定ビット長と等しいブロック長を有する転置情報を前記受信装置の公開鍵により暗号化した暗号化転置情報を生成し、通信メッセージの先頭ビットから前記乱数の所定ビット長に等しい長さの各ビットにより構成された第1の領域の通信メッセージに対しては、前記転置情報に基づいて、これらの各ビットを前記乱数の所定ビット長と等しいブロック長の転置を施した転置メッセージの各ビットと、前記乱数の先頭ビットから所定ビット長までの各ビットと、をそれぞれ互いに排他的論理和演算することにより、第1の暗号化メッセージを生成し、前記乱数の所定ビット長を超える前記通信メッセージの各ビットから構成された第2の領域の通信メッセージに対しては、前記転置情報に基づいて、これらの各ビットを前記転置のブロック長の単位毎に転置を施した転置メッセージの各ビットと、前記通信メッセージの該ビット位置から前記乱数の所定ビット長を減じたビット位置の前記通信メッセージの各ビットと、をそれぞれ互いに排他的論理和演算することにより、第2の暗号化メッセージを生成し、前記暗号化乱数と前記暗号化転置情報と第1及び第2の暗号化メッセージとを接続して、送信装置から受信装置へ通信し、前記受信装置は、自らの秘密鍵により、前記暗号化乱数及び前記暗号化転置情報からそれぞれ前記乱数及び前記転置情報を復号化し、第1の暗号化メッセージに対しては、これらの各ビットと、前記乱数の先頭ビットから所定ビット長までの各ビットと、をそれぞれ互いに排他的論理和演算して得られた転置メッセージに前記転置の逆写像の転置を施して第1の領域の通信メッセージを復号化し、第2の暗号化メッセージに対しては、これらの各ビットと、該ビット位置から前記乱数の所定ビット長を減じたビット位置の前記通信メッセージの各ビットと、をそれぞれ互いに排他的論理和演算して得られた転置メッセージに前記転置の逆写像の転置を施して第2の領域の通信メッセージを復号化する、ことを要旨とするストリーム暗号による通信方法である。

【0048】また請求項14記載の発明は、請求項12または請求項13に記載のストリーム暗号による通信方法において、前記乱数のビット数は、前記公開鍵暗号に

より1度に暗号化可能なビット数を超えるビット数であり、それぞれ複数回の暗号化及び復号化によって前記乱数の暗号化及び復号化が行われることを要旨とする。

【0049】また請求項15記載の発明は、それぞれ乱数発生器を備えた送信装置と受信装置との間で、公開鍵暗号を用いる暗号化通信により、乱数発生アルゴリズム及びまたは乱数の初期値を共有することにより、双方の乱数発生器から所定ビット長の同一の乱数を発生させ、前記送信装置は、前記乱数の所定ビット長と等しいブロック長を有する転置情報を前記受信装置の公開鍵により暗号化した暗号化転置情報を生成し、通信メッセージの先頭ビットから前記乱数の所定ビット長に等しい長さの各ビットにより構成された第1の領域の通信メッセージに対しては、前記転置情報に基づいて、これらの各ビットを前記乱数の所定ビット長と等しいブロック長の転置を施した転置メッセージの各ビットと、前記乱数の先頭ビットから所定ビット長までの各ビットと、をそれぞれ互いに排他的論理和演算することにより、第1の暗号化メッセージを生成し、前記乱数の所定ビット長を超える前記通信メッセージの各ビットから構成された第2の領域の通信メッセージに対しては、前記転置情報に基づいて、これらの各ビットを前記転置のブロック長の単位毎に転置を施した転置メッセージの各ビットと、前記通信メッセージの該ビット位置から前記乱数の所定ビット長を減じたビット位置の前記通信メッセージの各ビットと、をそれぞれ互いに排他的論理和演算することにより、第2の暗号化メッセージを生成し、前記暗号化転置情報と第1の暗号化メッセージと第2の暗号化メッセージとを接続して前記送信装置から前記受信装置へ通信し、前記受信装置は、自らの秘密鍵により前記暗号化転置情報から転置情報を復号化し、第1の暗号化メッセージに対しては、これらの各ビットと、前記乱数の先頭ビットから所定ビット長までの各ビットと、をそれぞれ互いに排他的論理和演算して得られた転置メッセージに前記転置の逆写像の転置を施して第1の領域の通信メッセージを復号化し、第2の暗号化メッセージに対しては、これらの各ビットと、該ビット位置から前記乱数の所定ビット長を減じたビット位置の前記通信メッセージの各ビットと、をそれぞれ互いに排他的論理和演算して得られた転置メッセージに前記転置の逆写像の転置を施して第2の領域の通信メッセージを復号化する、ことを要旨とするストリーム暗号による通信方法である。

【0050】また請求項16記載の発明は、請求項15に記載のストリーム暗号による通信方法において、前記送信装置及び受信装置にそれぞれ備えられた乱数発生器から、発生される乱数の周期を超えて、それぞれ乱数を取り出すことを要旨とする。

【0051】また請求項17記載の発明は、通信メッセージの先頭から所定のビット長を第1の領域の通信メッセージとし、前記通信メッセージの所定のビット長を超

える部分を第2の領域の通信メッセージとする通信メッセージの分割を行い、第1の領域の通信メッセージに対しては公開鍵暗号により、第2の領域の通信メッセージに対してはストリーム暗号により、それぞれ送信装置から受信装置へ通信する通信方法であって、前記送信装置は、前記乱数の所定ビット長と等しいブロック長を有する転置情報を前記受信装置の公開鍵により暗号化した暗号化転置情報を生成し、第1の領域の通信メッセージを前記転置情報に基づいて転置した第1の転置メッセージを前記受信装置の公開鍵により暗号化して、第1の暗号化メッセージを生成し、第2の領域の通信メッセージに該当する前記分割前の通信メッセージの各ビットに対しては、前記転置情報に基づいて、これらの通信メッセージを構成する各ビットを前記転置のブロック長の単位毎に転置を施した第2の転置メッセージの各ビットと、前記通信メッセージの該ビット位置から前記乱数の所定ビット長を減じたビット位置の第1の通信メッセージの各ビットと、をそれぞれ互いに排他的論理和演算することにより、第2の暗号化メッセージを生成し、前記暗号化転置情報と第1の暗号化メッセージと第2の暗号化メッセージとを接続して送信し、前記受信装置は、自らの秘密鍵により、前記暗号化転置情報及び第1の暗号化メッセージからそれぞれ前記転置情報及び第1の転置メッセージを復号化し、この第1の転置メッセージに前記転置の逆写像の転置を施して第1の領域の通信メッセージを復号化し、第2の暗号化メッセージの各ビットに対しては、これらの各ビットと、該ビット位置が対応する通信メッセージのビット位置から前記所定のビット長を減じたビット位置の復号化された通信メッセージの各ビットと、をそれぞれ互いに排他的論理和演算することにより、第2の領域の通信メッセージを復号化する、ことを要旨とするストリーム暗号による通信方法である。

【0052】また請求項18記載の発明は、請求項17に記載のストリーム暗号による通信方法において、前記第1の領域の通信メッセージのビット数は、前記公開鍵暗号により1度に暗号化可能なビット数を超えるビット数であり、それぞれ複数回の暗号化及び復号化によって第1の領域の通信メッセージの暗号化及び復号化が行われることを要旨とする。

【0053】請求項10ないし請求項18のいずれかに記載の発明によれば、請求項1ないし請求項9のいずれかに記載のストリーム暗号による通信方式において、さらに通信メッセージに対して転置を行うことにより、さらに安全強度を高めることができる。

【0054】また請求項19記載の発明は、請求項1ないし請求項18のいずれか1項に記載のストリーム暗号による通信方法において、前記排他的論理和演算を行う処理を、複数ビット並列して実行させることを要旨とする。

【0055】また請求項20記載の発明は、請求項1な

いし請求項 19 のいずれか 1 項に記載のストリーム暗号による通信方法において、前記第 2 の領域の通信メッセージを暗号化または復号化するための排他的論理和演算の処理は、少なくとも一方の演算対象データを前記第 1 の領域の通信メッセージのビット数だけシフトする動作を含むことを要旨とする。

【0056】また請求項 21 記載の発明は、送信装置と受信装置との間で所定のビット長の乱数を共有させる乱数共有化手段と、通信メッセージの先頭ビットから前記乱数の所定ビット長に等しい長さの各ビットに対しては、前記乱数の先頭ビットから所定ビット長までの各ビットと排他的論理和演算し、前記乱数の所定ビット長を超える前記通信メッセージの各ビットに対しては、該ビット位置から前記乱数の所定ビット長を減じたビット位置の前記通信メッセージの各ビットと排他的論理和演算することにより暗号化メッセージを生成する暗号化手段を備えた送信装置と、前記暗号化メッセージの先頭ビットから前記乱数の所定ビット長に等しい長さの各ビットに対しては、前記乱数の先頭ビットから所定ビット長までの各ビットと排他的論理和演算し、前記乱数の所定ビット長を超える前記暗号化メッセージの各ビットに対しては、該ビット位置から前記乱数の所定ビット長を減じたビット位置の前記暗号化メッセージの各ビットと排他的論理和演算することにより復号化メッセージを得る復号化手段を備えた受信装置と、を備えたことを要旨とするストリーム暗号による通信システムである。

【0057】また請求項 22 記載の発明は、請求項 21 に記載のストリーム暗号による通信システムにおいて、前記乱数共有化手段は、前記送信装置と前記受信装置との間で、それぞれ個別に生成された異なる乱数に基づいて生成された情報を互いに交換し、この交換された情報及び前記個別に生成された異なる乱数に基づいて、前記送信装置及び前記受信装置がそれぞれ同一の共有乱数を生成するものであることを要旨とする。

【0058】また請求項 23 記載の発明は、請求項 21 に記載のストリーム暗号による通信システムにおいて、前記乱数共有化手段は、前記受信装置の公開鍵により公開鍵暗号化された乱数を送信装置より送信する公開鍵暗号化手段と、この公開鍵暗号化された乱数を受信し受信装置自身の秘密鍵により乱数を復号化する公開鍵復号化手段と、を備えたものであることを要旨とする。

【0059】また請求項 24 記載の発明は、請求項 21 に記載のストリーム暗号による通信システムにおいて、前記乱数共有化手段は、前記送信装置に設けられた乱数発生アルゴリズム及びまたは乱数の初期値を設定可能な第 1 の乱数発生器と、前記乱数発生アルゴリズム及びまたは乱数の初期値を前記受信装置の公開鍵により公開鍵暗号化する公開鍵暗号化手段と、この公開鍵暗号化された乱数発生アルゴリズム及びまたは乱数の初期値を受信装置自身の秘密鍵により復号化する公開鍵復号化手段

と、前記受信装置に設けられ、この復号化された乱数発生アルゴリズム及びまたは乱数の初期値を設定可能な第 2 の乱数発生器と、を備えたことを要旨とする。

【0060】また請求項 25 記載の発明は、それぞれ乱数の初期値を構成するビットの値が外部より設定される複数ビットのシフトレジスタと、このシフトレジスタの各ビットから新たな乱数を生成するためのビットを指定するための値が乱数発生アルゴリズムとして外部より設定される制御レジスタと、前記制御レジスタの値により指定されたシフトレジスタのビット間で排他的論理和演算を行い、その結果をシフトレジスタに入力する排他的論理和回路と、を備えた乱数発生器を送信装置及び受信装置がそれぞれ備えてなり、両装置の乱数発生器が互いに等しい乱数を生成することを特徴とするストリーム暗号による通信システムである。

【0061】また請求項 26 記載の発明は、請求項 21 に記載のストリーム暗号による通信システムにおいて、前記送信装置は、転置情報に基づいて、前記乱数の所定ビット長に等しいブロック長を有するブロック単位に前記通信メッセージのビット位置を入れ替える第 1 の転置手段と、前記転置情報を受信装置の公開鍵により暗号化し暗号化転置情報を生成する公開鍵暗号化手段と、をさらに備えてなり、前記受信装置は、自身の秘密鍵により前記暗号化転置情報を復号化し転置情報を生成する公開鍵復号化手段と、この復号化された転置情報に基づいて、該転置情報の示す転置の逆写像を前記復号化メッセージに施す第 2 の転置手段と、を備えたことを要旨とする。

【0062】また請求項 27 記載の発明は、請求項 21 に記載のストリーム暗号による通信システムにおいて、前記暗号化手段または前記復号化手段は、共有乱数が初期状態として設定されるとともにシフトイン入力に通信メッセージまたは暗号化メッセージの直列供給源が接続されたシフトレジスタと、このシフトレジスタのシフトアウト出力に一方の入力が接続され、前記通信メッセージまたは暗号化メッセージの直列供給源に他方の入力が接続され、その出力が暗号化メッセージまたは復号化された通信メッセージとなる 2 入力排他的論理和回路と、を備えたことを要旨とする。

【0063】また請求項 28 記載の発明は、請求項 27 に記載のストリーム暗号による通信システムにおいて、前記シフトレジスタまたは該シフトレジスタ及び前記排他的論理和回路を備えた回路が単一の集積回路に集積化されたことを要旨とする。

【0064】また請求項 29 記載の発明は、請求項 21 に記載のストリーム暗号による通信システムにおいて、前記暗号化手段及びまたは前記復号化手段は、前記排他的論理和演算を複数ビット並列に行う演算器を備えたことを要旨とする。

【0065】また請求項 30 記載の発明は、所定のビッ

10

20

30

40

50

ト幅で順次供給される第1のデータを一時保持する第1の保持手段と、前記所定のビット幅の第2のデータまたは第1の保持手段に保持されたデータを一時保持する第2の保持手段と、第1及び第2の保持手段の内容をそれぞれビット毎に排他的論理和演算を行う前記所定ビット幅の並列演算器と、を備えた回路を単一の集積回路に集積化したことを要旨とするストリーム暗号による通信システムである。

【0066】本発明では、従来方式に比較して、暗号化および復号化の処理量が少ないので、リアルタイム性のあるマルチメディア情報の効果的な秘匿通信を行なうことができる。また、大量ファイルの暗号転送においても有効である。

【0067】

【発明の実施の形態】次に、図面を参照して本発明の実施の形態を詳細に説明する。図1は、本発明に係るストリーム暗号による通信システムの第1の実施形態を示すシステム構成図であり、請求項1または請求項2記載の発明に対応する。同図において、通信システム11は、乱数共有化部21と、送信装置31と、受信装置51と、通信路71とを備えて構成されている。

【0068】乱数共有化部21は、送信装置31と受信装置51とに、所定のビット長 k の互いに等しい乱数（乱数列とも呼ばれる） R を秘密に共有させるものである。これには、例えば、乱数 R を記憶させたフロッピーディスクを書留便で郵送することも可能である。

【0069】なお、以下の説明においては、特に断らない限り、乱数 R はビット長 k の2進乱数とし、その i 番目のビットの値を $R[i]$ とする。

【0070】また、通信メッセージであるビット長 N の平文 M は、その第1の領域である先頭ビット $M[1]$ から同 k ビット目である $M[k]$ までの先頭ブロック（以下、このブロックを $M1,k$ とも記す）と、第2の領域で

ある平文 M のビット $M[i]$ （ $k < i \leq N$ ）からなる後続ブロックとに便宜上分割して説明する。

【0071】送信装置31は、平文 M からその先頭ブロック $M1,k$ を切り出す先頭ブロック切り出し処理部111と、先頭ブロック $M1,k$ を暗号化する先頭ブロック暗号化処理部131と、この先頭ブロックに続くビット $M[i]$ （ $k < i \leq N$ ）を暗号化する後続ブロック暗号化処理部151と、先頭ブロック暗号化処理部131により生成された第1の暗号化メッセージ及び後続ブロック暗号化処理部151により生成された第2の暗号化メッセージを接続して1つの暗号文として通信路71へ送出する暗号文接続処理部171と、を備えて構成されている。

【0072】受信装置51は、通信路71を介して受信された暗号文から、第1及び第2の暗号化メッセージを分離する暗号文分離処理部271と、第1の暗号化メッセージから平文の先頭ブロックを復号化する先頭ブロック復号化処理部231と、第2の暗号化メッセージから平文の後続ブロックを復号化する後続ブロック復号化処理部251と、それぞれ復号化された先頭ブロック及び後続ブロックを接続して平文 M を復元するビット接続処理部211とを備えて構成されている。

【0073】次に、送信装置31の動作をフローチャート及びメモリ割付を示す表を参照して詳細に説明する。図9は、送信装置31の暗号化送信処理を説明するフローチャートであり、表1は同処理におけるメモリ上のデータ配置を示す表である。なお、表1及び以下の各表において、ビット位置を示すカウンタ i の値によってデータ内容が異なる場合、データ内容欄を複数設けている。そしてデータ内容欄の「←」印は、左側のデータ内容欄と同一の内容であることを示す。

【0074】

【表1】

データ番号	データ内容 ($1 \leq i \leq k$)	データ内容 ($k < i$)
1	平文 M	←
2	乱数 R	←
3	乱数 R のビット長 k	←
4	カウンタ i	←
5	$R[i]$	$M[i-k]$
6	$M[i]$	←
7	$C[i] \equiv R[i] (+) M[i]$	$C[i] \equiv M[i-k] (+) M[i]$

表1に示すように暗号化送信処理においては、平文 M 、乱数 R がそれぞれデータ番号1、2に与えられる。

【0075】図9において、まず共有乱数 R のビット長 k が、データ番号3に格納される（ステップS101）。次いで、暗号化すべき平文のビット位置を示すカウンタ i を初期設定するために、データ番号4に1を格

納する（ステップS103）。

【0076】次いで、 i が k 以下がどうかを判定し（ステップS105）、 $i \leq k$ ならば、暗号化すべき平文のビット位置 i は、通信メッセージの第1の領域であるので、乱数 R の i ビット目 $R[i]$ を取り出してデータ番号5に格納し、平文 M の i ビット目 $M[i]$ を取り出

し、データ番号6に格納し、

$$C[i] \equiv R[i] (+) M[i] \quad 1 \leq i \leq k \text{ のとき} \quad \dots (10)$$

式(10)により暗号化を行い、 $C[i]$ をデータ番号7に格納する(ステップS107)。ここで、 $(+)$ は、排他的論理和を表し、 $C[i]$ は、暗号化メッセージの*i*ビット目を示している。

【0077】ステップS105の判定において、 $i > k$ であれば、暗号化すべき平文のビット位置*i*は、通信メ

$$C[i] \equiv M[i-k] (+) M[i] \quad k < i \text{ のとき} \quad \dots (11)$$

式(11)により暗号化を行い、 $C[i]$ をデータ番号7に格納する(ステップS109)。

【0078】次いで、データ番号7の $C[i]$ を送信し(ステップS111)、次いで、メッセージが終了したかどうか($i = N$)を判定し(ステップS113)、終了していなければ($i \neq N$)、*i*を1だけ増加させて(ステップS115)、ステップS105に戻る。 $i = N$ ならば終了する。

【0079】なお、終了判定条件として最終ビット番号*N*が与えられるとしたが、マルチメディア情報等の暗号化されるデータの性質によっては、予め最終ビット番号

【数9】

ッセージの第2の領域であるので、平文*M*の*i-k*ビット目 $M[i-k]$ を取り出してデータ番号5に格納し、平文*M*の*i*ビット目 $M[i]$ を取り出してデータ番号6に格納し、

【数10】

10 が得られず、別途設定される終了フラグ等を参照して終了しても良い。これは、受信装置51における復号化や他の実施の形態においても同様である。

【0080】次に、受信装置51の動作をフローチャート及びメモリ割付を示す表を参照して詳細に説明する。図10は、受信装置51の受信復号化処理を説明するフローチャートであり、表2は同処理におけるメモリ上のデータ配置を示す表である。

【0081】

【表2】

データ番号	データ内容 ($1 \leq i \leq k$)	データ内容 ($k < i$)
1	暗号文 C	←
2	乱数 R	←
3	乱数 <i>R</i> のビット長 k	←
4	カウンタ i	←
5	$R[i]$	$M[i-k]$
6	$C[i]$	←
7	$M[i] \equiv R[i] (+) C[i]$	$M[i] \equiv M[i-k] (+) C[i]$
8	平文 M	←

表2に示すように受信復号化処理においては、暗号文*C*、乱数*R*がそれぞれデータ番号1、2に与えられる。

【0082】図10において、まず共有乱数*R*のビット長*k*が、データ番号3に格納される(ステップS121)。次いで、復号化すべき暗号文のビット位置を示すカウンタ*i*を初期設定するために、データ番号4に1を格納する(ステップS123)。

$$M[i] \equiv R[i] (+) C[i] \quad 1 \leq i \leq k \text{ のとき} \quad \dots (12)$$

式(12)により復号化を行い、 $M[i]$ をデータ番号7に格納する(ステップS127)。

【0084】ステップS125の判定において、 $i > k$ であれば、復号化すべき暗号文のビット位置*i*は、平文*M*の第2の領域であるので、平文*M*の*i-k*ビット目 M

$$M[i] \equiv M[i-k] (+) C[i] \quad k < i \text{ のとき} \quad \dots (13)$$

式(13)により復号化を行い、 $M[i]$ をデータ番号7に格納する(ステップS129)。

【0085】次いで、データ番号7の $M[i]$ をデータ番号8の平文*M*の末尾に接続して格納し(ステップS131)、次いで、暗号文が終了したかどうか($i = N$)

【0083】次いで、*i*が*k*以下かどうかを判定し(ステップS125)、 $i \leq k$ ならば、復号化すべき暗号文のビット位置*i*は、通信メッセージの第1の領域であるので、乱数*R*の*i*ビット目 $R[i]$ を取り出してデータ番号5に格納し、暗号文*C*の*i*ビット目 $C[i]$ を取り出してデータ番号6に格納し、

【数11】

10 $[i-k]$ を取り出してデータ番号5に格納し、暗号文*C*の*i*ビット目 $C[i]$ を取り出し、データ番号6に格納し、

【数12】

を判定し(ステップS133)、終了していなければ($i \neq N$)、*i*を1だけ増加させて(ステップS135)、ステップS125に戻る。 $i = N$ ならば、終了する。

【0086】また、第2の実施形態として、図1の乱数

共有化部 21 は、請求項 2 に記載のように、公開鍵配送法により、前記乱数 R を共有させるものであってもよい。この公開鍵配送法には、例えば、DH 型公開鍵配送法やその変形を利用することができる。

【0087】図 2 は、本発明に係るストリーム暗号による通信システムの第 3 の実施形態を示すシステム構成図であり、請求項 3 記載の発明に対応する。同図において、通信システム 12 は、送信装置 32 と、受信装置 52 と、通信路 71、72 とを備えて構成されている。

【0088】送信装置 32 は、所定ビット長 k の乱数 R を発生させる乱数生成処理部 311 と、乱数 R を受信装置 52 の公開鍵 e により暗号化した暗号化乱数 $e(R)$ を通信路 72 に送出する乱数暗号化処理部 331 と、平文 M からその先頭ブロック $M1, k$ を切り出す先頭ブロック切り出し処理部 111 と、先頭ブロック $M1, k$ を暗号化する先頭ブロック暗号化処理部 131 と、この先頭ブロックに続くビット $M[i]$ ($k < i \leq N$) を暗号化する後続ブロック暗号化処理部 151 と、先頭ブロック暗号化処理部 131 により生成された第 1 の暗号化メッセージ及び後続ブロック暗号化処理部 151 により生成された第 2 の暗号化メッセージを接続して 1 つの暗号文として通信路 71 へ送出する暗号文接続処理部 171 と、を備えて構成されている。

【0089】受信装置 52 は、通信路 72 を介して受信された暗号化乱数 $e(R)$ を自らの秘密鍵 d で復号化して乱数 R を得る乱数復号化処理部 351 と、通信路 71 を介して受信された暗号文から、第 1 及び第 2 の暗号化メッセージを分離する暗号文分離処理部 271 と、第 1 の暗号化メッセージから平文の先頭ブロックを復号化する先頭ブロック復号化処理部 231 と、第 2 の暗号化メッセージから平文の後続ブロックを復号化する後続ブロック復号化処理部 251 と、それぞれ復号化された先頭ブロック及び後続ブロックを接続して平文 M を復元するビット接続処理部 211 とを備えて構成されている。

【0090】本第 2 の実施の形態と第 1 の実施の形態との主要な相違は、送信装置 32 と受信装置 52 との間に、乱数暗号化処理部 331、通信路 72 及び乱数復号化処理部 351 からなる公開鍵暗号方式の暗号化通信手段を備えており、平文 M のストリーム暗号化通信に先だって、共有すべき乱数 R が公開鍵暗号方式で伝送されることである。

【0091】この公開鍵暗号の持つ安全性によって、ストリーム暗号の秘密鍵である乱数 R を配送する際の安全性が確保される。また、乱数 R を伝送するための公開鍵暗号方式としては、特に限定されないが、例えば、RSA 型暗号、ラビン型暗号等が利用できる。以下に説明する他の実施の形態においても、同様な公開鍵暗号を利用することができる。また、公開鍵 e による暗号化関数を $e(\cdot)$ 、秘密鍵 d による復号化関数を $d(\cdot)$ とす

る。

【0092】図 3 は、本発明に係るストリーム暗号による通信システムの第 4 の実施形態を示すシステム構成図であり、請求項 4 記載の発明に対応する。同図において、通信システム 13 は、送信装置 33 と、受信装置 53 と、通信路 71 とを備えて構成されている。

【0093】送信装置 33 は、所定ビット長 k の乱数 R を発生させる乱数生成処理部 311 と、乱数 R を受信装置 53 の公開鍵 e により暗号化した暗号化乱数 $e(R)$ を生成する乱数暗号化処理部 331 と、平文 M からその先頭ブロック $M1, k$ を切り出す先頭ブロック切り出し処理部 111 と、先頭ブロック $M1, k$ を暗号化する先頭ブロック暗号化処理部 131 と、この先頭ブロックに続くビット $M[i]$ ($k < i \leq N$) を暗号化する後続ブロック暗号化処理部 151 と、暗号化乱数 $e(R)$ 及び先頭ブロック暗号化処理部 131 により生成された第 1 の暗号化メッセージ及び後続ブロック暗号化処理部 151 により生成された第 2 の暗号化メッセージを接続して 1 つの暗号文として通信路 71 へ送出する暗号文接続処理部 172 と、を備えて構成されている。

【0094】受信装置 53 は、通信路 71 を介して受信された暗号文から、暗号化乱数 $e(R)$ 及び第 1、第 2 の暗号化メッセージをそれぞれ分離する暗号文分離処理部 272 と、暗号化乱数 $e(R)$ を自らの秘密鍵 d で復号化して乱数 $R = d(e(R))$ を得る乱数復号化処理部 351 と、第 1 の暗号化メッセージから平文の先頭ブロックを復号化する先頭ブロック復号化処理部 231 と、第 2 の暗号化メッセージから平文の後続ブロックを復号化する後続ブロック復号化処理部 251 と、それぞれ復号化された先頭ブロック及び後続ブロックを接続して平文 M を復元するビット接続処理部 211 とを備えて構成されている。

【0095】本実施の形態と第 3 の実施の形態との主要な相違は、暗号化乱数 $e(R)$ と平文 M をストリーム暗号化した暗号文 C が接続されて、一つの暗号文 $e(R) \parallel C$ として通信路 71 を介して送信されることである。なお、記号「 \parallel 」は、その左右に表記されたデータの接続を示すものとする。

【0096】本実施の形態においても、共有すべき乱数 R が公開鍵暗号方式で伝送されることにより、公開鍵暗号の持つ安全性によって、ストリーム暗号の秘密鍵である乱数 R を配送する際の安全性が確保される。

【0097】次に、送信装置 33 の動作をフローチャート及びメモリ割付を示す表を参照して詳細に説明する。図 11 は、送信装置 33 の暗号化送信処理を説明するフローチャートであり、表 3 は同処理におけるメモリ上のデータ配置を示す表である。

【0098】

【表 3】

35		36	
データ番号	データ内容 (1 ≤ i ≤ k)	データ内容 (k < i)	
1	公開鍵 n	←	
2	公開鍵 e	←	
3	平文 M	←	
4	乱数 R	←	
5	乱数 R のビット長 k	←	
6	e (R)	←	
7	カウンタ i	←	
8	R [i]	M [i-k]	
9	M [i]	←	
1 0	C [i] ≡ R [i] (+) M [i]	C [i] ≡ M [i-k] (+) M [i]	

表 3 に示すように、送信装置 3 3 における暗号化送信処理においては、初期状態として、受信装置 5 3 の公開鍵 n、e 及び平文 M がそれぞれデータ番号 1、2 及び 3 に与えられている。

【0099】図 1 1 において、まず乱数生成処理部 3 1 1 が生成した乱数 R がデータ番号 4 に格納される（ステップ S 1 4 1）。次いでデータ番号 1、2 の公開鍵 n、e により乱数 R を暗号化して、暗号化乱数 e (R) を生成してデータ番号 6 に格納する（ステップ S 1 4 3）。次いで、e (R) を送信装置 3 3 から受信装置 5 3 へ送る（ステップ S 1 4 5）。

【0100】次いで、乱数 R のビット長 k がデータ番号 5 に格納される（ステップ S 1 4 7）。

【0101】次いで、暗号化すべき平文 M のビット位置を示すカウンタ i を初期設定するために、データ番号 7 に 1 を格納する（ステップ S 1 0 3）。次いで、i が k 以下かどうかを判定し（ステップ S 1 0 5）、i ≤ k ならば、暗号化すべき平文のビット位置 i は、通信メッセージの第 1 の領域であるので、乱数 R の i ビット目 R [i] を取り出してデータ番号 8 に格納し、平文 M の i ビット目 M [i] を取り出し、データ番号 9 に格納し、前記式 (1 0) により暗号化を行い、C [i] をデータ番号 1 0 に格納する（ステップ S 1 0 7）。ここで、(+) は、排他的論理和を表し、C [i] は、暗号化メッセージの i ビット目を示している。

【0102】ステップ S 1 0 5 の判定において、i > k であれば、暗号化すべき平文のビット位置 i は、通信メッセージの第 2 の領域であるので、平文 M の i - k ビット目 M [i - k] を取り出してデータ番号 8 に格納し、平文 M の i ビット目 M [i] を取り出してデータ番号 9 に格納し、前記式 (1 1) により暗号化を行い、C [i] をデータ番号 1 0 に格納する（ステップ S 1 0 9）。

【0103】次いで、データ番号 1 0 の C [i] を送信し（ステップ S 1 1 1）、次いで、メッセージが終了したかどうか (i = N) を判定し（ステップ S 1 1 3）、終了していなければ (i ≠ N)、i を 1 だけ増加させて（ステップ S 1 1 5）、ステップ S 1 0 5 に戻る。i = N ならば終了する。

【0104】なお、図 1 1 のステップ S 1 0 3 以下の処理は、メモリ上のデータの割付が異なるだけで、第 1 の実施形態を示す図 9 の対応するステップ番号と同じ処理内容である。

【0105】次に、受信装置 5 3 の動作をフローチャート及びメモリ割付を示す表を参照して詳細に説明する。図 1 2 は、受信装置 5 3 の受信復号化処理を説明するフローチャートであり、表 4 は同処理におけるメモリ上のデータ配置を示す表である。

【0106】

【表 4】

データ番号	データ内容 ($1 \leq i \leq k$)	データ内容 ($k < i$)
1	公開鍵 n	←
2	秘密鍵 d	←
3	暗号文 $e(R) \parallel C$	←
4	乱数 R	←
5	乱数 R のビット長 k	←
6	カウンタ i	←
7	$R[i]$	$M[i-k]$
8	$C[i]$	←
9	$M[i] \equiv R[i] (+) C[i]$	$M[i] \equiv M[i-k] (+) C[i]$
10	平文 M	←

表4に示すように、受信装置53の受信復号化处理においては、公開鍵 n 及び秘密鍵 d がそれぞれデータ番号1、2に与えられている。

【0107】図12において、まず暗号文 $e(R) \parallel C$ が受信され、データ番号3に格納される(ステップS161)。次いで、データ番号3の内容から暗号化乱数 $e(R)$ が切り出され、残りの暗号文 C がデータ番号3に格納される(ステップS163)。次いで、データ番号1及び2から読み出された受信装置53自身の公開鍵 n と秘密鍵 d により $d(e(R))$ を計算することにより乱数 R が復号化され、得られた乱数 R がデータ番号4に格納される(ステップS165)。次いで、乱数 R のビット長 k がデータ番号5に格納される(ステップS167)。

【0108】次いで、復号化すべき暗号文のビット位置を示すカウンタ i を初期設定するために、データ番号6に1を格納する(ステップS123)。次いで、 i が k 以下かどうかを判定し(ステップS125)、 $i \leq k$ ならば、復号化すべき暗号文のビット位置 i は、通信メッセージの第1の領域であるので、乱数 R の i ビット目 $R[i]$ を取り出してデータ番号7に格納し、暗号文 C の i ビット目 $C[i]$ を取り出してデータ番号8に格納し、前記式(12)により復号化を行い、 $M[i]$ をデータ番号9に格納する(ステップS127)。

【0109】ステップS125の判定において、 $i > k$ であれば、復号化すべき暗号文のビット位置 i は、平文 M の第2の領域であるので、平文 M の $i-k$ ビット目 $M[i-k]$ を取り出してデータ番号7に格納し、暗号文 C の i ビット目 $C[i]$ を取り出し、データ番号8に格納し、前記式(13)により復号化を行い、 $M[i]$ をデータ番号9に格納する(ステップS129)。

【0110】次いで、データ番号7の $M[i]$ をデータ番号8の平文 M の末尾に接続して格納し(ステップS131)、次いで、暗号文が終了したかどうか($i=N$)を判定し(ステップS133)、終了していなければ($i \neq N$)、 i を1だけ増加させて(ステップS13

5)、ステップS125に戻る。 $i=N$ ならば、終了する。

【0111】なお、図12のステップS123以下の処理は、メモリ上のデータの割付が異なるだけで、第1の実施形態を示す図11の対応するステップ番号と同じ処理内容である。

【0112】図4は、本発明に係るストリーム暗号による通信システムの第5の実施形態を示すシステム構成図であり、請求項5記載の発明に対応する。同図において、通信システム14は、送信装置34と、受信装置54と、通信路71とを備えて構成されている。

【0113】送信装置34は、所定ビット長 $k \times m$ (m は2以上の整数)の乱数 R を発生させる乱数生成処理部312と、この乱数 R をそれぞれ長さ k の m 個のブロック $R1, R2, \dots, Rm$ に分割する乱数ブロック分割処理部322と、受信装置54の公開鍵 e により各乱数ブロックを暗号化して暗号化乱数 $e(R1), e(R2), \dots, e(Rm)$ を生成する乱数暗号化処理部332と、平文 M からその先頭ブロック $M1, km$ を切り出す先頭ブロック切り出し処理部111と、先頭ブロック $M1, km$ を暗号化する先頭ブロック暗号化処理部131と、この先頭ブロックに続くビット $M[i]$ ($km < i \leq N$)を暗号化する後続ブロック暗号化処理部151と、暗号化乱数 $e(R1), e(R2), \dots, e(Rm)$ 及び先頭ブロック暗号化処理部131により生成された第1の暗号化メッセージ及び後続ブロック暗号化処理部151により生成された第2の暗号化メッセージを接続して1つの暗号文として通信路71へ送出する暗号文接続処理部173と、を備えて構成されている。

【0114】受信装置54は、通信路71を介して受信された暗号文から、暗号化乱数 $e(R1), e(R2), \dots, e(Rm)$ 及び第1、第2の暗号化メッセージをそれぞれ分離する暗号文分離処理部273と、暗号化乱数 $e(R1), e(R2), \dots, e(Rm)$ を自らの秘密鍵 d で復号化して各乱数ブロック $R1, R2, \dots, Rm$ を得る乱数復号化処理部352と、各乱数ブロック $R1, R2, \dots, Rm$ を接続して乱数

Rを復元する乱数ブロック接続処理部362と、第1の暗号化メッセージから平文の先頭ブロックを復号化する先頭ブロック復号化処理部231と、第2の暗号化メッセージから平文の後続ブロックを復号化する後続ブロック復号化処理部251と、それぞれ復号化された先頭ブロック及び後続ブロックを接続して平文Mを復元するビット接続処理部211とを備えて構成されている。

【0115】本第5の実施の形態と図3に示した第4の実施の形態との相違は、乱数Rのビット長がkのm倍に拡張されていることであり、乱数Rを暗号化するために、これをm個のブロックに分割して、それぞれ暗号化していることである。これにより暗号文接続処理部173で接続された暗号文は、 $e(R_1) \parallel \dots \parallel e(R_m) \parallel C$ となる。

【0116】この暗号化に対応して、暗号文分離処理部273は、m個のブロックからなる暗号化乱数をそれぞれ

れ分離し、乱数復号化処理部352に供給する。乱数復号化処理部352でそれぞれ復号化された分割乱数は、乱数ブロック接続処理部362で接続され、元の乱数Rが復元される。

【0117】本実施の形態においても、共有すべき乱数Rが公開鍵暗号方式で伝送されることにより、公開鍵暗号の持つ安全性によって、ストリーム暗号の秘密鍵である乱数Rを配送する際の安全性が確保される。

【0118】次に、送信装置34の動作をフローチャート及びメモリ割付を示す表を参照して詳細に説明する。図13は、送信装置34の暗号化送信処理を説明するフローチャートであり、表5は同処理におけるメモリ上のデータ配置を示す表である。

【0119】

【表5】

データ番号	データ内容 ($1 \leq i \leq km$)	データ内容 ($km < i$)
1	公開鍵 n	←
2	公開鍵 e	←
3	平文 M	←
4	ビット長 k	←
5	ブロック数 m	←
6	乱数 R	←
7	分割乱数 R_1	←
...	...	←
$6+m$	分割乱数 R_m	←
$7+m$	暗号化乱数 $e(R_1)$	←
...	...	←
$6+2m$	暗号化乱数 $e(R_m)$	←
$7+2m$	カウンタ i	←
$8+2m$	$R[i]$	$M[i-km]$
$9+2m$	$M[i]$	←
$10+2m$	$C[i] \equiv R[i](+)M[i]$	$C[i] \equiv M[i-km](+)M[i]$

表5に示すように、送信装置34における暗号化送信処理においては、初期状態として、受信装置54の公開鍵n、e及び平文Mがそれぞれデータ番号1、2及び3に与えられている。また、乱数Rを分割すべきブロック数mがデータ番号5に与えられている。

【0120】図13において、まず乱数生成処理部312が生成した乱数Rがデータ番号6に格納される（ステップS181）。次いで、乱数Rがそれぞれkビット毎のm個の分割乱数 R_1, R_2, \dots, R_m に分割されて、それぞれデータ番号7から $6+m$ に格納される（ステップS183）。

【0121】次いで、データ番号1、2の公開鍵n、eにより各分割乱数 R_1, R_2, \dots, R_m を暗号化して、暗号化

乱数 $e(R_1), e(R_2), \dots, e(R_m)$ を生成し、データ番号 $7+m$ から $6+2m$ に格納する（ステップS185）。次いで、暗号化乱数 $e(R_1), e(R_2), \dots, e(R_m)$ を送信装置34から受信装置54へ送る（ステップS187）。

【0122】次いで、分割乱数 R_j のビット長kがデータ番号4に格納される（ステップS189）。次いで、暗号化すべき平文Mのビット位置を示すカウンタiを初期設定するために、データ番号 $7+2m$ に1を格納する（ステップS191）。次いで、iが $k \times m$ 以下かどうかを判定し（ステップS193）、 $i \leq km$ ならば、暗号化すべき平文のビット位置iは、通信メッセージの第1の領域であるので、乱数Rのiビット目 $R[i]$ を取

り出してデータ番号 $8 + 2m$ に格納し、平文 M の i ビット目 $M[i]$ を取り出し、データ番号 $9 + 2m$ に格納

$$C[i] \equiv R[i] (+) M[i]$$

式(14)により暗号化を行い、 $C[i]$ をデータ番号 $10 + 2m$ に格納する(ステップS195)。ここで、 $(+)$ は、排他的論理和を表し、 $C[i]$ は、暗号化メッセージの i ビット目を示している。

【0123】ステップS193の判定において、 $i > k \times m$ であれば、暗号化すべき平文のビット位置 i は、通

$$C[i] \equiv M[i - km] (+) M[i]$$

式(15)により暗号化を行い、 $C[i]$ をデータ番号 $10 + 2m$ に格納する(ステップS197)。

【0124】次いで、データ番号 $10 + 2m$ の $C[i]$ を送信し(ステップS199)、次いで、メッセージが終了したかどうか($i = N$)を判定し(ステップS201)、終了していなければ($i \neq N$)、 i を1だけ増加させて(ステップS203)、ステップS193に戻る。 $i = N$ ならば終了する。

データ番号	データ内容 ($1 \leq i \leq km$)	データ内容 ($km < i$)
1	公開鍵 n	←
2	秘密鍵 d	←
3	暗号文 $e(R1) \parallel \dots e(Rm) \parallel C$	←
4	分割乱数 $R1$	←
...	...	←
$3 + m$	分割乱数 Rm	←
$4 + m$	乱数 R	←
$5 + m$	ビット長 k	←
$6 + m$	ブロック数 m	←
$7 + m$	カウンタ i	←
$8 + m$	$R[i]$	$M[i - km]$
$9 + m$	$C[i]$	←
$10 + m$	$M[i] \equiv R[i] (+) C[i]$	$M[i] \equiv M[i - km] (+) C[i]$
$11 + m$	平文 M	←

表6に示すように、受信装置54の受信復号化処理においては、公開鍵 n 及び秘密鍵 d がそれぞれデータ番号1、2に与えられている。

【0127】図14において、まず暗号文 $e(R1) \parallel \dots e(Rm) \parallel C$ が受信され、データ番号3に格納される(ステップS221)。次いで、データ番号3の内容から暗号化乱数 $e(R1)$ 、 $e(R2)$ 、 \dots 、 $e(Rm)$ がそれぞれひとつずつ切り出され、残りの暗号文がデータ番号3に格納される(ステップS223)。

【0128】次いで、データ番号1及び2から読み出された受信装置54自身の公開鍵 n と秘密鍵 d により暗号化乱数 $e(R1)$ 、 $e(R2)$ 、 \dots 、 $e(Rm)$ が復号化され、得られた分割乱数 $R1$ 、 $R2$ 、 \dots 、 Rm がデータ番号4から $3 + m$ に格納される(ステップS225)。次いで、分割乱数

し、

【数13】

$$1 \leq i \leq km \text{ のとき } \dots (14)$$

信メッセージの第2の領域であるので、平文 M の $i - km$ ビット目 $M[i - km]$ を取り出してデータ番号 $8 + 2m$ に格納し、平文 M の i ビット目 $M[i]$ を取り出してデータ番号 $9 + 2m$ に格納し、

【数14】

$$km < i \text{ のとき } \dots (15)$$

【0125】次に、受信装置54の動作をフローチャート及びメモリ割付を示す表を参照して詳細に説明する。図12は、受信装置54の受信復号化処理を説明するフローチャートであり、表6は同処理におけるメモリ上のデータ配置を示す表である。

【0126】

【表6】

$R1$ 、 $R2$ 、 \dots 、 Rm が順次連接され、元の乱数 R が復元されて、データ番号 $4 + m$ に格納される(ステップS227)。次いで分割乱数 Rj のビット長 k がデータ番号 $5 + m$ に格納される(ステップS229)。

【0129】次いで、復号化すべき暗号文のビット位置を示すカウンタ i を初期設定するために、データ番号 $7 + m$ に1を格納する(ステップS231)。次いで、 i が $k \times m$ 以下かどうかを判定し(ステップS233)、 $i \leq k \times m$ ならば、復号化すべき暗号文のビット位置 i は、通信メッセージの第1の領域であるので、乱数 R の i ビット目 $R[i]$ を取り出してデータ番号 $8 + m$ に格納し、暗号文 C の i ビット目 $C[i]$ を取り出してデータ番号 $9 + m$ に格納し、

【数15】

43

$$M[i] \equiv R[i] (+) C[i]$$

式(16)により復号化を行い、 $M[i]$ をデータ番号 $10+m$ に格納する(ステップS235)。

【0130】ステップS233の判定において、 $i > k \times m$ であれば、復号化すべき暗号文のビット位置 i は、平文 M の第2の領域であるので、平文 M の $i - km$ ビット

$$M[i] \equiv M[i - km] (+) C[i]$$

式(17)により復号化を行い、 $M[i]$ をデータ番号 $10+m$ に格納する(ステップS237)。

【0131】次いで、データ番号 $10+m$ の $M[i]$ をデータ番号 $11+m$ の平文 M の末尾に接続して格納し

(ステップS239)、次いで、暗号文が終了したかどうか($i = N$)を判定し(ステップS241)、終了していなければ($i \neq N$)、 i を1だけ増加させて(ステップS243)、ステップS233に戻る。 $i = N$ ならば、終了する。

【0132】図5は、本発明に係るストリーム暗号による通信システムの第6の実施形態を示すシステム構成図であり、請求項6または7記載の発明に対応する。同図において、通信システム15は、送信装置35と、受信装置55と、通信路71、72とを備えて構成されている。

【0133】送信装置35は、乱数発生アルゴリズムH及び乱数初期値 $R0$ を生成する乱数パラメータ生成処理部343と、乱数発生アルゴリズムH及び乱数初期値 $R0$ に従って乱数 R を発生させる乱数生成処理部313と、乱数発生アルゴリズムH及び乱数初期値 $R0$ を受信装置55の公開鍵 e により暗号化した暗号化パラメータ $e(H, R0)$ を通信路72に送出する乱数パラメータ暗号化処理部333と、平文 M からその先頭ブロック $M1, k$ を切り出す先頭ブロック切り出し処理部111と、先頭ブロック $M1, k$ を暗号化する先頭ブロック暗号化処理部131と、この先頭ブロックに続くビット $M[i]$ ($k < i \leq N$)を暗号化する後続ブロック暗号化処理部151と、先頭ブロック暗号化処理部131により生成された第1の暗号化メッセージ及び後続ブロック暗号化処理部151により生成された第2の暗号化メッセージを接続して1つの暗号文として通信路71へ送出する暗号文接続処理部171と、を備えて構成されている。

【0134】なお、先頭ブロック切り出し処理部111、先頭ブロック暗号化処理部131、後続ブロック暗号化処理部151、及び暗号文接続処理部171は、図2に示した前記第3の実施の形態と同様であるので、同じ符号を付与して詳細な説明を省略する。

【0135】受信装置55は、通信路72を介して受信された暗号化パラメータ $e(H, R0)$ を自らの秘密鍵 d で復号化して乱数発生アルゴリズムH及び乱数初期値 $R0$ を得る乱数パラメータ復号化処理部353と、復号化された乱数発生アルゴリズムH及び乱数初期値 $R0$ が設定されることにより送信装置35が生成する乱数と等

(23)

特開平10-84339

44

$$1 \leq i \leq km \text{ のとき } \dots (16)$$

と目 $M[i - km]$ を取り出してデータ番号 $8+m$ に格納し、暗号文 C の i ビット目 $C[i]$ を取り出し、データ番号 $9+m$ に格納し、

【数16】

$$km < i \text{ のとき } \dots (17)$$

しい乱数を生成する乱数生成処理部313と、通信路71を介して受信された暗号文から、第1及び第2の暗号化メッセージを分離する暗号文分離処理部271と、第1の暗号化メッセージから平文の先頭ブロックを復号化する先頭ブロック復号化処理部231と、第2の暗号化メッセージから平文の後続ブロックを復号化する後続ブロック復号化処理部251と、それぞれ復号化された先頭ブロック及び後続ブロックを接続して平文 M を復元するビット接続処理部211とを備えて構成されている。

【0136】なお、暗号文分離処理部271、先頭ブロック復号化処理部231、後続ブロック復号化処理部251、及びビット接続処理部211は、図2に示した前記第3の実施の形態と同様であるので、同じ符号を付与して詳細な説明を省略する。

【0137】本第6の実施の形態と、図2に示した前記第3の実施の形態との主要な相違は、送信装置35及び受信装置55がそれぞれ乱数生成処理部313を備えていて、送信装置35から受信装置55へ、乱数発生アルゴリズムH及び乱数の初期値 $R0$ を公開鍵暗号方式により乱数発生アルゴリズムH及び乱数初期値 $R0$ を伝送することにより、双方の乱数生成処理部313から互いに等しい乱数を生成し、乱数を共有するものである。また、乱数発生アルゴリズムH及び乱数初期値 $R0$ を伝送する公開鍵暗号の持つ安全性によって、ストリーム暗号の秘密鍵である乱数 R の安全性が確保される。

【0138】図15は、本第6の実施の形態における乱数共有化の動作を説明するフローチャートである。乱数共有化以外の動作は図2に示した前記第3の実施の形態と同様であるので説明を省略する。

【0139】まず、送信側では、乱数発生アルゴリズムH及び乱数初期値 $R0$ を乱数パラメータとして生成する(ステップS261)。次いで、送信装置35の乱数生成処理部313に、乱数発生アルゴリズムH及び乱数初期値 $R0$ を設定する(ステップS263)。次いで、受信装置55の公開鍵 e により、乱数発生アルゴリズムH及び乱数初期値 $R0$ を暗号化して暗号化パラメータ $e(H, R0)$ を生成し(ステップS265)、通信路72を介して受信装置55へ送信する(ステップS267)。次いで、送信装置35の乱数生成処理部313が設定された乱数発生アルゴリズムH及び乱数初期値 $R0$ に従って乱数 R を生成する(ステップS269)。

【0140】次に、受信側では、暗号化パラメータ $e(H, R0)$ を受信し(ステップS271)、自らの秘

密鍵 d により暗号化パラメータ e (H, R_0) を復号化して、乱数発生アルゴリズム H 及び乱数初期値 R_0 を得る (ステップ $S273$)。次いで、受信装置 55 の乱数生成処理部 313 に、乱数発生アルゴリズム H 及び乱数初期値 R_0 を設定する (ステップ $S275$)。次いで、受信装置 35 の乱数生成処理部 313 が設定された乱数発生アルゴリズム H 及び乱数初期値 R_0 に従って乱数 R を生成する (ステップ $S277$)。

【0141】こうして送信装置 35 と受信装置 55 との間で、乱数発生アルゴリズム H 及び乱数初期値 R_0 を共有することにより双方で互いに等しい乱数 R を発生させ、それぞれストリーム暗号の暗号化鍵及び復号化鍵に使用することができる。

【0142】なお、乱数発生アルゴリズムは、いずれのアルゴリズムを利用してもよいが、例えば、線形合同法

$$R[n] = h_p R[n-1] + h_{p-1} R[n-2] + \dots + h_1 R[n-p] \pmod{2} \quad \dots (19)$$

式 (19) に示す漸化式で乱数のビット列が生成される。

【0145】この場合は、乱数発生アルゴリズム $H \equiv h_1, h_2, \dots, h_p$ 、及び p ビットからなる乱数初期値 $R_0 \equiv R[1], R[2], \dots, R[p]$ を適当な暗号化により送信装置から受信装置へ伝送することにより、双方の装置で互いに等しい乱数を共有することができる。

【0146】図 6 は、本発明に係るストリーム暗号による通信システムの第 7 の実施形態を示すシステム構成図であり、請求項 8 記載の発明に対応する。同図において、通信システム 16 は、送信装置 36 と、受信装置 56 と、通信路 71 とを備えて構成されている。

【0147】送信装置 36 は、平文 M からその先頭ブロック $M_{1,k}$ を切り出す先頭ブロック切り出し処理部 111 と、先頭ブロック $M_{1,k}$ を受信装置 56 の公開鍵 e により暗号化する先頭ブロック暗号化処理部 141 と、この先頭ブロックに続くビット $M[i]$ ($k < i \leq N$) を暗号化する後続ブロック暗号化処理部 151 と、先頭ブロック暗号化処理部 141 により生成された第 1 の暗号化メッセージ及び後続ブロック暗号化処理部 151 により生成された第 2 の暗号化メッセージを接続して 1 つの暗号文として通信路 71 へ送出する暗号文連接処理部 174 と、を備えて構成されている。

【0148】受信装置 56 は、通信路 71 を介して受信された暗号文から、第 1、第 2 の暗号化メッセージをそれぞれ分離する暗号文分離処理部 274 と、第 1 の暗号

を利用するならば、そのアルゴリズムは、

【数 17】

$$X(n) = a \times X(n-1) + c \pmod{m} \quad \dots (18)$$

式 (18) に示す漸化式で非負整数列を生成し、2 進数に変換する。

【0143】この場合、正整数 a, m 及び非負整数 c を乱数発生アルゴリズム H として、また $X(0)$ を乱数初期値 R_0 として、適当な暗号化により送信装置から受信装置へ伝送することにより、双方の装置で互いに等しい乱数を共有することができる。

【0144】また、シフトレジスタ系列乱数または最大周期系列乱数を生成するとすれば、それぞれ 0 または 1 の値をもつ h_i ($1 \leq i \leq p$) を係数として、

【数 18】

化メッセージ $e(M_{1,k})$ を自らの秘密鍵 d で復号化して平文の先頭ブロック $M_{1,k}$ を得る先頭ブロック復号化処理部 241 と、第 2 の暗号化メッセージから平文の後続ブロックを復号化する後続ブロック復号化処理部 251 と、それぞれ復号化された先頭ブロック及び後続ブロックを接続して平文 M を復元するビット連接処理部 211 とを備えて構成されている。

【0149】本実施の形態と図 3 に示した第 4 の実施の形態との主要な相違は、所定ビット長の乱数 R の代わりに、平文の先頭ブロック $M_{1,k}$ をパッドとして用いるとともに、平文の先頭ブロック $M_{1,k}$ を受信装置の公開鍵により暗号化して送信することである。

【0150】本実施の形態においては、通信メッセージの第 1 の領域である平文の先頭ブロック $M_{1,k}$ を第 2 の領域のパッドとするとともに、先頭ブロック $M_{1,k}$ が公開鍵暗号方式で伝送されることにより、公開鍵暗号の持つ安全性によって、ストリーム暗号の秘密鍵であるパッドを配送する際の安全性が確保される。

【0151】次に、送信装置 36 の動作をフローチャート及びメモリ割付を示す表を参照して詳細に説明する。図 16 は、送信装置 36 の暗号化送信処理を説明するフローチャートであり、表 7 は同処理におけるメモリ上のデータ配置を示す表である。

【0152】

【表 7】

データ番号	データ内容
1	公開鍵 n
2	公開鍵 e
3	平文 M
4	メッセージブロック $M1, k$
5	メッセージブロック $M1, k$ のビット長 k
6	$e(M1, k)$
7	カウンタ i
8	$M[i-k]$
9	$M[i]$
10	$C[i] \equiv M[i-k](+)M[i] \quad (k < i)$

表7に示すように、送信装置36における暗号化送信処理においては、初期状態として、受信装置56の公開鍵 n 、 e 及び平文 M がそれぞれデータ番号1、2及び3に与えられている。

【0153】図16において、まずデータ番号3に格納された平文 M から、通信メッセージの第1の領域である先頭の k ビットからなるメッセージブロック $M1, k$ が切り出され、データ番号4に格納される(ステップS301)。次いで、メッセージブロック $M1, k$ のビット長 k がデータ番号5に格納される(ステップS303)。

【0154】次いでデータ番号1、2の公開鍵 n 、 e によりメッセージブロック $M1, k$ を暗号化して、 $e(M1, k)$ を生成してデータ番号6に格納する(ステップS305)。次いで、 $e(M1, k)$ を送信する(ステップS307)。次いで、暗号化すべき平文 M のビット位置を示すカウンタ i を初期設定するために、データ番号7に $k+1$ を格納する(ステップS309)。平文 M のビット位置 i が $i > k$ の範囲は全て平文 M の第2の領域であ

る。次いで、平文 M の $i-k$ ビット目 $M[i-k]$ を取り出してデータ番号8に格納し、平文 M の i ビット目 $M[i]$ を取り出してデータ番号9に格納し、前記式(11)により暗号化を行い、 $C[i]$ をデータ番号10に格納する(ステップS311)。

【0155】次いで、データ番号10の $C[i]$ を送信し(ステップS313)、次いで、メッセージが終了したかどうか($i=N$)を判定し(ステップS315)、終了していなければ($i \neq N$)、 i を1だけ増加させて(ステップS317)、ステップS311に戻る。 $i=N$ ならば終了する。

【0156】次に、受信装置56の動作をフローチャート及びメモリ割付を示す表を参照して詳細に説明する。図17は、受信装置56の受信復号化処理を説明するフローチャートであり、表8は同処理におけるメモリ上のデータ配置を示す表である。

【0157】

【表8】

データ番号	データ内容
1	公開鍵 n
2	秘密鍵 d
3	暗号文 $e(M1, k) \parallel C$
4	メッセージブロック $M1, k$
5	メッセージブロック $M1, k$ のビット長 k
6	カウンタ i
7	$M[i-k]$
8	$C[i]$
9	$M[i] \equiv M[i-k](+)C[i] \quad (k < i)$
10	平文 M

表8に示すように、受信装置56の受信復号化処理においては、公開鍵 n 及び秘密鍵 d がそれぞれデータ番号1、2に与えられている。

【0158】図17において、まず暗号文 $e(M1, k)$

$\parallel C$ が受信され、データ番号3に格納される(ステップS321)。次いで、データ番号3の内容から暗号文 $e(M1, k)$ が切り出され、残りの暗号文 C がデータ番号3に格納される(ステップS323)。

【0159】次いで、データ番号1及び2から読み出された受信装置56自身の公開鍵 n と秘密鍵 d により暗号文 $e(M1, k)$ が復号化され、得られたメッセージ(平文)の先頭ブロック $M1, k$ がデータ番号4に格納される(ステップS325)。次いで、先頭ブロック $M1, k$ のビット長 k がデータ番号5に格納される(ステップS327)。

【0160】次いで、復号化すべき暗号文 C のビット位置を示すカウンタ i を初期設定するために、データ番号6に $k+1$ を格納する(ステップS329)。なお本実施の形態においては、復号化すべき暗号文 C のビット位置 i は、全て平文 M の第2の領域である。

【0161】次いで、平文 M の $i-k$ ビット目 $M[i-k]$ を取り出してデータ番号7に格納し、暗号文 C の i ビット目 $C[i]$ を取り出し、データ番号8に格納し、前記式(13)により復号化を行い、 $M[i]$ をデータ番号9に格納する(ステップS331)。

【0162】次いで、データ番号7の $M[i]$ をデータ番号8の平文 M の末尾に接続して格納し(ステップS333)、次いで、暗号文が終了したかどうか($i=N$ か否か)を判定し(ステップS335)、終了していなければ($i \neq N$)、 i を1だけ増加させて(ステップS337)、ステップS331に戻る。 $i=N$ ならば、終了する。

【0163】図7は、本発明に係るストリーム暗号による通信システムの第8の実施形態を示すシステム構成図であり、請求項9記載の発明に対応する。同図において、通信システム17は、送信装置37と、受信装置57と、通信路71とを備えて構成されている。

【0164】送信装置37は、平文 M の先頭から k ビット毎に m (m は2以上の整数)個のブロック $M1$ 、 $M2$ 、 \dots 、 Mm を切り出す前部ブロック切り出し処理部112と、前部ブロック $M1$ 、 $M2$ 、 \dots 、 Mm を受信装置57の公開鍵 e によりそれぞれ暗号化する前部ブロック暗号化処理部142と、この前部ブロックに続くビット $M[i]$ ($k+m < i \leq N$)を暗号化する後続ブロック暗号化処理部152と、前部ブロック暗号化処理部142により生成された第1の暗号化メッセージ $e(M1)$ 、 $e(M2)$ 、 \dots 、 $e(Mm)$ 及び後続ブロック暗号化処理部152により生成された第2の暗号化メッセージ C とを連

接して1つの暗号文 $e(M1) \parallel e(M2) \parallel \dots \parallel e(Mm) \parallel C$ として通信路71へ送出する暗号文接続処理部175と、を備えて構成されている。

【0165】受信装置57は、通信路71を介して受信された暗号文から、第1、第2の暗号化メッセージをそれぞれ分離する暗号文分離処理部275と、第1の暗号化メッセージ $e(M1)$ 、 $e(M2)$ 、 \dots 、 $e(Mm)$ を自らの秘密鍵 d で復号化して平文の m 個の前部ブロック $M1$ 、 $M2$ 、 \dots 、 Mm を得る前部ブロック復号化処理部242と、第2の暗号化メッセージから平文の後続ブロックを復号化する後続ブロック復号化処理部252と、それぞれ復号化された前部ブロック及び後続ブロックを接続して平文 M を復元するビット接続処理部212とを備えて構成されている。

【0166】本実施の形態と図6に示した第7の実施の形態との主要な相違は、第7の実施形態が平文の先頭ブロック $M1, k$ をパッドとして用いるとともに、平文の先頭ブロック $M1, k$ を受信装置の公開鍵により暗号化して送信しているのに対し、本実施の形態では、平文 M の前部を構成するそれぞれ k ビットからなる m 個のブロックをパッドとして用いるとともに、 m 回の公開鍵暗号化により m 個のブロックを暗号化して送信することである。

【0167】これにより1回に公開鍵暗号化可能な k ビットを超える十分に長い前部ブロックをパッドとすることができ、後続ブロックのストリーム暗号化の強度をさらに高めることができる。

【0168】本実施の形態においても、通信メッセージの第1の領域である平文の前部ブロック $M1$ 、 $M2$ 、 \dots 、 Mm を第2の領域のパッドとするとともに、前部ブロック $M1$ 、 $M2$ 、 \dots 、 Mm が公開鍵暗号方式で伝送されることにより、公開鍵暗号の持つ安全性によって、ストリーム暗号の秘密鍵であるパッドを配送する際の安全性が確保される。

【0169】次に、送信装置37の動作をフローチャート及びメモリ割付を示す表を参照して詳細に説明する。図18は、送信装置37の暗号化送信処理を説明するフローチャートであり、表9は同処理におけるメモリ上のデータ配置を示す表である。

【0170】

【表9】

データ番号	データ内容
1	公開鍵 n
2	公開鍵 e
3	平文 M
4	公開鍵暗号化ブロックのビット長 k
5	公開鍵暗号化ブロックのブロック数 m
6	$M_1 = M_1, k$
...	...
$5 + m$	$M_m = M_{k(m-1)+1, km}$
$6 + m$	$e(M_1)$
...	...
$5 + 2m$	$e(M_m)$
$6 + 2m$	カウンタ i
$7 + 2m$	$M[i - km]$
$8 + 2m$	$M[i]$
$9 + 2m$	$C[i] \equiv M[i - km](+)M[i] \quad (km < i)$

表 9 に示すように、送信装置 3 7 における暗号化送信処理においては、初期状態として、受信装置 5 7 の公開鍵 n 、 e 及び平文 M がそれぞれデータ番号 1、2 及び 3 に与えられている。また公開鍵暗号化ブロックのビット長 k 及び公開鍵暗号化される平文 M の前部ブロック数 m がそれぞれデータ番号 4、5 に与えられる。

【0171】図 18 において、まず平文 M から切り出すメッセージブロックを計数するカウンタ j を 1 に初期設定する（ステップ S 3 4 1）。次いで、データ番号 4 より公開鍵暗号化ブロックのビット長 k を読出し作業変数 30 に設定する（ステップ S 3 4 3）。

【0172】次いで、データ番号 3 の平文 M の先頭から k ビットのブロック M_j を切り出し、データ番号 $5 + j$ に格納する（ステップ S 3 4 5）。次いで、データ番号 $5 + j$ の平文ブロック M_j を受信装置 5 7 の公開鍵 e により暗号化し、得られた $e(M_j)$ をデータ番号 $5 + m + j$ に格納する（ステップ S 3 4 7）。

【0173】次いで、 $e(M_j)$ を送信し（ステップ S 3 4 9）、公開鍵暗号化するブロック数が終了したか否かを判定するため j と m とを比較する（ステップ S 3 5 1）。

【0174】ステップ S 3 5 1 の比較において、 $j \neq m$ であれば j に 1 を加えて（ステップ S 3 5 3）、ステップ S 3 4 5 に戻る。 $j = m$ であれば、暗号化すべき平文

M のビット位置を示すカウンタ i を初期設定するために、データ番号 $6 + 2m$ に $km + 1$ を格納する（ステップ S 3 5 5）。平文 M のビット位置 i が $i > k \times m$ の範囲は全て平文 M の第 2 の領域である。

【0175】次いで、平文 M の $i - km$ ビット目 $M[i - km]$ を取り出してデータ番号 $7 + 2m$ に格納し、平文 M の i ビット目 $M[i]$ を取り出してデータ番号 $8 + 2m$ に格納し、前記式 (15) により暗号化を行い、 $C[i]$ をデータ番号 $9 + 2m$ に格納する（ステップ S 3 5 7）。

【0176】次いで、データ番号 $9 + 2m$ の $C[i]$ を送信し（ステップ S 3 5 9）、次いで、メッセージが終了したかどうか ($i = N$) を判定し（ステップ S 3 6 1）、終了していなければ ($i \neq N$)、 i を 1 だけ増加させて（ステップ S 3 6 3）、ステップ S 3 5 7 に戻る。 $i = N$ ならば終了する。

【0177】次に、受信装置 5 7 の動作をフローチャート及びメモリ割付を示す表を参照して詳細に説明する。図 19 は、受信装置 5 7 の受信復号化処理を説明するフローチャートであり、表 10 は同処理におけるメモリ上のデータ配置を示す表である。

【0178】

【表 10】

データ番号	データ内容
1	公開鍵 n
2	秘密鍵 d
3	暗号文 $e(M_1) \parallel \dots \parallel e(M_m) \parallel C$
4	公開鍵暗号化ブロックのビット長 k
5	公開鍵暗号化ブロックのブロック数 m
6	$M_1 = M_1, k$
...	...
$5+m$	$M_m = M_k(m-1) + 1, km$
$6+m$	カウンタ i
$7+m$	$M[i-km]$
$8+m$	$C[i]$
$9+m$	$M[i] \equiv M[i-km](+)C[i] \quad (km < i)$
$10+m$	平文 M

表 10 に示すように、受信装置 57 の受信復号化処理においては、公開鍵 n 及び秘密鍵 d がそれぞれデータ番号 1、2 に与えられている。また、公開鍵暗号化ブロックのビット長 k 及び公開鍵暗号化により通信される平文 M の前部ブロック数 m がそれぞれデータ番号 4、5 に与えられる。

【0179】図 19 において、まず暗号文 $e(M_1) \parallel e(M_2) \parallel \dots \parallel e(M_m) \parallel C$ が受信され、データ番号 3 に格納される（ステップ S371）。次いで、暗号文から切り出すメッセージブロックを計数するカウンタ j を 1 に初期設定する（ステップ S373）。次いで、データ番号 4 より公開鍵暗号化ブロックのビット長 k を読出して作業変数に設定する（ステップ S375）。

【0180】次いで、データ番号 3 の暗号文の先頭から k ビットのブロック $e(M_j)$ を切り出し、残りの暗号文をデータ番号 3 に格納する（ステップ S377）。次いで、データ番号 1 及び 2 から読み出された受信装置 56 自身の公開鍵 n と秘密鍵 d により暗号文 $e(M_j)$ が復号化され、得られた平文のブロック M_j がデータ番号 $5+j$ に格納される（ステップ S379）。

【0181】次いで、公開鍵暗号化されたブロック数が終了したか否かを判定するため j と m とを比較する（ステップ S381）。ステップ S381 の比較において、 $j \neq m$ であれば j に 1 を加えて（ステップ S383）、ステップ S377 に戻る。 $j = m$ であれば、復号化すべき暗号文 C のビット位置を示すカウンタ i を初期設定するために、データ番号 $6+m$ に $km+1$ を格納する（ステップ S329）。なお本実施の形態においては、復号化すべき暗号文 C のビット位置 i は、全て平文 M の第 2 の領域である。

【0182】次いで、平文 M の $i-km$ ビット目 $M[i-km]$ を取り出してデータ番号 $7+m$ に格納し、暗号文 C の i ビット目 $C[i]$ を取り出し、データ番号 $8+$

m に格納し、前記式 (17) により復号化を行い、 $M[i]$ をデータ番号 $9+m$ に格納する（ステップ S387）。

【0183】次いで、データ番号 $9+m$ の $M[i]$ をデータ番号 $10+m$ の平文 M の末尾に接続して格納し（ステップ S389）、次いで、暗号文が終了したかどうか（ $i = N$ ）を判定し（ステップ S391）、終了していなければ（ $i \neq N$ ）、 i を 1 だけ増加させて（ステップ S393）、ステップ S387 に戻る。 $i = N$ ならば、終了する。

【0184】図 8 は、本発明に係るストリーム暗号による通信システムの第 9 の実施形態を示すシステム構成図であり、転置を含む暗号化の代表として請求項 15 記載の発明に対応する。同図において、通信システム 18 は、送信装置 38 と、受信装置 58 と、通信路 71 とを備えて構成されている。

【0185】送信装置 38 は、所定ビット長 k の乱数 R を発生させる乱数生成処理部 311 と、乱数 R を受信装置 58 の公開鍵 e により暗号化した暗号化乱数 $e(R)$ を生成する乱数暗号化処理部 331 と、前記乱数の所定ビット長 k に等しいビット長のブロックに対する転置 T を生成する転置情報生成処理部 411 と、この転置 T を受信装置 58 の公開鍵 e により暗号化した暗号化転置 $e(T)$ を生成する転置情報暗号化処理部 421 と、平文 M からその先頭ブロック M_1, k を切り出す先頭ブロック切り出し処理部 111 と、先頭ブロック M_1, k を乱数 R 及び転置 T を利用して暗号化する先頭ブロック暗号化処理部 133 と、この先頭ブロックに続くビット $M[i]$ （ $k < i \leq N$ ）を先頭ブロック M_1, k 及び転置 T を利用して暗号化する後続ブロック暗号化処理部 153 と、暗号化乱数 $e(R)$ 及び暗号化転置 $e(T)$ 及び先頭ブロック暗号化処理部 133 により生成された第 1 の暗号化メッセージ及び後続ブロック暗号化処理部 153 により

生成された第2の暗号化メッセージを接続して1つの暗号文 $e(R) \parallel e(T) \parallel C$ として通信路71へ送出する暗号文接続処理部176と、を備えて構成されている。

【0186】受信装置58は、通信路71を介して受信された暗号文から、暗号化乱数 $e(R)$ 及び暗号化転置 $e(T)$ 及び第1、第2の暗号化メッセージをそれぞれ分離する暗号文分離処理部276と、暗号化乱数 e

(R) を自らの秘密鍵 d で復号化して乱数 R を得る乱数復号化処理部351と、暗号化転置 $e(T)$ を自らの秘密鍵 d で復号化して転置 T を得る転置情報復号化処理部431と、転置 T からその逆写像 T^{-1} を生成する逆写像生成処理部441と、第1の暗号化メッセージから平文の先頭ブロックを復号化する先頭ブロック復号化処理部233と、第2の暗号化メッセージから平文の後続ブロックを復号化する後続ブロック復号化処理部253と、それぞれ復号化された先頭ブロック及び後続ブロックを接続して平文 M を復元するビット接続処理部211とを備えて構成されている。

【0187】本実施の形態で用いる k ビット長のブロックの転置 T は、巡回置換の積で表示することができる。例えば、 $k=5$ とするとき、5ビットの転置 $T = \{1 \rightarrow$

$3, 2 \rightarrow 4, 3 \rightarrow 5, 4 \rightarrow 2, 5 \rightarrow 1\}$ は、 $T = (1, 3, 5)(2, 4)$ と表示することができる。

【0188】本実施の形態と図3に示した第4の実施の形態との主要な相違は、平文 M のビットが転置 T により転置されたのちストリーム暗号化されることと、この転置情報を公開鍵暗号化して暗号化転置 $e(T)$ が送信装置から受信装置へ送られ、転置情報を復号化した受信装置は、復号化されたストリーム暗号に対して転置 T の逆写像である T^{-1} を施して平文 M を復元することである。

【0189】本実施の形態においては、暗号化の過程に転置を加えることにより、さらに解読を困難とし、安全性を高めることができる。また共有すべき乱数 R 及び転置 T が公開鍵暗号方式で伝送されることにより、公開鍵暗号の持つ安全性によって、秘密鍵である乱数 R 及び転置 T を配送する際の安全性が確保される。

【0190】次に、送信装置38の動作をフローチャート及びメモリ割付を示す表を参照して詳細に説明する。図20は、送信装置38の暗号化送信処理を説明するフローチャートであり、表11は同処理におけるメモリ上のデータ配置を示す表である。

【0191】

【表11】

データ番号	データ内容 ($1 \leq i \leq k$)	データ内容 ($k < i$)
1	公開鍵 n	←
2	公開鍵 e	←
3	平文 M	←
4	乱数 R	←
5	乱数 R のビット長 k	←
6	暗号化乱数 $e(R)$	←
7	転置 T	←
8	暗号化転置 $e(T)$	←
9	カウンタ i	←
10	$R[i]$	$M[i-k]$
11	$M[i]$	←
12	$C[i] \equiv R[i](+)T * M[i]$	$C[i] \equiv M[i-k](+)T * M[i]$

表11に示すように、送信装置38における暗号化送信処理においては、初期状態として、受信装置58の公開鍵 n 、 e 及び平文 M がそれぞれデータ番号1、2及び3に与えられている。

【0192】図20において、まず乱数生成処理部311が乱数 R を生成し、この乱数 R をデータ番号4に格納する(ステップS401)。次いでデータ番号1、2の公開鍵 n 、 e により乱数 R を暗号化し、暗号化乱数 $e(R)$ をデータ番号6に格納するとともに、 $e(R)$ を送信装置38から受信装置58へ送信する(ステップS403)。

【0193】次いで、乱数 R のビット長 k をデータ番号

5に格納する(ステップS405)。

【0194】次いで、転置情報生成処理部411が転置 T を生成し、この転置 T をデータ番号7に格納する(ステップS407)。次いでデータ番号1、2の公開鍵 n 、 e により転置 T を暗号化し、暗号化転置 $e(T)$ をデータ番号8に格納するとともに、 $e(T)$ を送信装置38から受信装置58へ送信する(ステップS409)。

【0195】次いで、暗号化すべき平文 M のビット位置を示すカウンタ i を初期設定するために、データ番号9に1を格納する(ステップS411)。次いで、 i が k 以下かどうかを判定し(ステップS413)、 $i \leq k$ な

らば、暗号化すべき平文のビット位置 i は、通信メッセージの第1の領域であるので、乱数 R の i ビット目 $R[i]$ を取り出してデータ番号10に格納し、平文 M の i ビット目 $M[i]$ を取り出し、データ番号11に格納し、

【数19】

$$C[i] \equiv R[i](+) T * M[i] \quad \dots (20)$$

式(20)により暗号化を行い、 $C[i]$ をデータ番号12に格納する(ステップS415)。ここで、 $T * M[i]$ は平文 M の i ビット目 $M[i]$ に転置 T を施す処理を表し、 $(+)$ は排他的論理和を表し、 $C[i]$ は暗号化メッセージの i ビット目を表している。

【0196】ステップS413の判定において、 $i > k$ であれば、暗号化すべき平文のビット位置 i は、通信メッセージの第2の領域であるので、平文 M の $i - k$ ビット目 $M[i - k]$ を取り出してデータ番号10に格納し、平文 M の i ビット目 $M[i]$ を取り出してデータ番号11に格納し、

データ番号	データ内容 ($1 \leq i \leq k$)	データ内容 ($k < i$)
1	公開鍵 n	←
2	秘密鍵 d	←
3	暗号文 $e(R) \parallel e(T) \parallel C$	←
4	乱数 R	←
5	乱数 R のビット長 k	←
6	転置 T	←
7	ビットカウンタ i	←
8	ブロックカウンタ j	←
9	$R[i]$	$M[i - k]$
10	$C[i]$	←
11	$T * M[i] \equiv R[i](+) C[i]$	$T * M[i] \equiv M[i - k](+) C[i]$
12	$T * M_j$	←
13	$M_j \equiv T^{-1} * T * M_j$	←
14	平文 M	←

表12に示すように、受信装置58の受信復号化処理においては、公開鍵 n 及び秘密鍵 d がそれぞれデータ番号1、2に与えられている。

【0200】図21において、まず暗号文 $e(R) \parallel e(T) \parallel C$ が受信され、データ番号3に格納される(ステップS431)。次いで、データ番号3の内容から暗号化乱数 $e(R)$ が切り出され、残りの暗号文がデータ番号3に格納されるとともに、データ番号1及び2から読み出された受信装置58自身の公開鍵 n と秘密鍵 d により暗号化乱数 $e(R)$ が復号化され、得られた乱数 R がデータ番号4に格納される(ステップS433)。次いで、乱数 R のビット長 k がデータ番号5に格納される(ステップS435)。

【0201】次いで、データ番号3の内容から暗号化転

【数20】

$$C[i] \equiv M[i - k](+) T * M[i] \quad \dots (21)$$

式(21)により暗号化を行い、 $C[i]$ をデータ番号12に格納する(ステップS417)。

【0197】次いで、データ番号12の $C[i]$ を送信し(ステップS419)、次いで、メッセージが終了したかどうか($i = N$)を判定し(ステップS421)、終了していなければ($i \neq N$)、 i を1だけ増加させて(ステップS423)、ステップS413に戻る。 $i = N$ ならば終了する。

【0198】次に、受信装置58の動作をフローチャート及びメモリ割付を示す表を参照して詳細に説明する。図21は、受信装置58の受信復号化処理を説明するフローチャートであり、表12は同処理におけるメモリ上のデータ配置を示す表である。

【0199】

【表12】

置 $e(T)$ が切り出され、残りの暗号文がデータ番号3に格納されるとともに、データ番号1及び2から読み出された受信装置58自身の公開鍵 n と秘密鍵 d により暗号化転置 $e(T)$ が復号化され、得られた転置 T がデータ番号6に格納される(ステップS437)。次いで、逆写像生成処理部441により転置 T の逆写像 T^{-1} が生成される(ステップS439)。

【0202】次いで、復号化すべき暗号文 C の k ビット毎のブロック番号を計数するカウンタ j と、暗号文 C のビット位置を示すカウンタ i を初期設定するために、データ番号7及び8にそれぞれ1を格納する(ステップS441)。次いで、 i が k 以下かどうかを判定し(ステップS443)、 $i \leq k$ ならば、復号化すべき暗号文のビット位置 i は、通信メッセージの第1の領域であるの

で、乱数Rのiビット目R[i]を取り出してデータ番号9に格納し、暗号文Cのiビット目C[i]を取り出してデータ番号10に格納し、

【数21】

$$T * M[i] \equiv R[i] (+) C[i] \quad \dots (22)$$

式(22)により復号化を行い、 $T * M[i]$ をデータ番号11に格納する(ステップS445)。

【0203】ステップS443の判定において、 $i > k$ となれば、最初のkビットのブロックの復号化が終わったので、このブロックに転置Tの逆写像 T^{-1} を行う($M_j \equiv T^{-1} * T * M_j$)ことにより、 M_j を復元し、データ番号13に格納するとともに、データ番号14の平文Mの末尾に接続して格納する(ステップS447)。

【0204】次いで、暗号文が終了したかどうかを判定し、終了していなければ、ブロック番号jを1だけ増加させて(ステップS453)、平文Mのi-kビット目 $M[i-k]$ を取り出してデータ番号9に格納し、暗号文Cのiビット目C[i]を取り出し、データ番号10に格納し、

【数22】

$$T * M[i] \equiv M[i-k] (+) C[i] \quad \dots (23)$$

式(13)により復号化を行い、 $T * M[i]$ をデータ番号11に格納する(ステップS455)。次いで、iがkの倍数か否かを判定し(ステップS457)、倍数でなければ、ビットカウンタiを1だけ増加して(ステップS459)、ステップS455へ戻る。iがkの倍数であれば、ステップS447へ戻り、kビットのブロック毎の転置 T^{-1} を行う。なお、ステップS447の転置 T^{-1} 処理が最後のブロックに対して行われると、その次の暗号文終了判定(ステップS451)で終了と判定され、受信復号化処理を終了する。

【0205】また、本実施の形態の変形例として、図6に記載したメッセージの先頭ブロックを公開鍵暗号化して送信するとともに、この先頭ブロックを後続ブロックのパッドとして利用する第7の実施の形態に転置を加えることができる。

【0206】この場合転置メッセージ $T * M$ の先頭のkビット長を $T * M1, k$ とし、 $T * M1, k$ を受信装置の公開鍵eで暗号化し、その結果を $e(T * M1, k)$ とする。また、 $i > k$ に対しては、 $C[i] \equiv M[i-k] (+) T * M[i]$ で暗号化する。送信装置は、接続された暗号文 $e(T) \parallel e(T * M1, k) \parallel C[k+1] \dots C[n]$ を受信装置へ送る。

【0207】受信装置は、まず $e(T)$ の部分から転置Tを復元する。次に、 $e(T * M1, k)$ の部分を、自らの秘密鍵で復号化し、 $T * M1, k$ を得る。さらに、この結果に転置Tの逆写像 T^{-1} を行ない、平文 $M1, k$ を復元する。次いで、 $i < k$ に対しては、 $T * M[i] \equiv M[i-k] (+) C[i]$ の演算を行なうことにより転置メッセージ $T * M[i]$ を得、さらに転置Tの逆写像 T^{-1} を行な

い、メッセージMを復元する。

【0208】図22は、乱数共有化部を除いた送信装置(a)および受信装置(b)の構成例を示す第10実施形態を示す回路図であり、請求項20及び請求項27に対応する。

【0209】図22(a)において、送信装置39は、kビットシフトレジスタ301と、排他的論理和回路303と、ビット送信回路305とを備えて構成されている。kビットシフトレジスタ301のシフトイン入力にはビット直列に供給される平文M[i]の信号が接続され、シフトアウト出力には、排他的論理和回路303の一方の入力が接続されている。排他的論理和回路303の他方の入力には、平文M[i]の信号が接続されている。排他的論理和回路303の出力は、ビット送信回路305を経て、通信路71へ接続されている。

【0210】次に、この送信装置39の動作を説明する。まず最初に、kビットシフトレジスタ301には、例えばkビットのパラレルロードパスからkビットの乱数Rが設定される。次いで、図示されないシフトクロックiに同期して平文Mのビット列M[i]が入力し始めると、シフトアウトからは、乱数Rのビット列R[i]が出力される。これにより、排他的論理和回路303の一方の入力には、R[i]が供給され、排他的論理和回路303の他方の入力には、平文M[i]が供給されるので、その出力は、第1の暗号化メッセージ $C[i] = R[i] (+) M[i]$ となる。ここで、(+)は排他的論理和演算を示す。この状態は、初期設定された乱数Rのkビット全てがシフトアウトするまで、即ち $1 \leq i \leq k$ の間継続する。

【0211】次いで、 $i = k + 1$ 以降のシフトクロックにおいては、シフトアウトデータは、シフトインデータのkビットタイム遅延したデータである $M[i-k]$ となるので、排他的論理和回路303の一方の入力には、 $M[i-k]$ が供給され、他方の入力にはM[i]が供給されるので、その出力は、第2の暗号化メッセージ $C[i] = M[i-k] (+) M[i]$ となる。

【0212】この送信装置39によれば、kビットの乱数Rが初期設定されるkビットシフトレジスタ301を用いることにより、シフトアウトデータは、 $R[i] \parallel M[i-k]$ となるので、通信メッセージの第1の領域と同第2の領域に対する処理が自動的に切り替わる。このため、特に第1の領域である先頭ブロックを切り出すことや、第1及び第2の暗号文を接続する必要がなく、簡単な回路構成で処理速度の高い暗号化装置を実現できる。

【0213】図22(b)において、受信装置59は、kビットシフトレジスタ301と、排他的論理和回路303と、ビット受信回路307とを備えて構成されている。

【0214】送信装置から送信された暗号文のビット列

10

20

30

40

50

C[i] は、通信路 71 及びビット受信回路 307 を介して k ビットシフトレジスタ 301 のシフトイン入力に接続されている。シフトアウト出力には、排他的論理和回路 303 の一方の入力が接続され、303 の他方の入力には、暗号文 C[i] の信号が接続されている。排他的論理和回路 303 の出力は、平文のビット列 M[i] を出力する。

【0215】次に、この受信装置 59 の動作を説明する。まず最初に、k ビットシフトレジスタ 301 には、例えば k ビットのパラレルロードパスから k ビットの乱数 R が設定される。次いで、図示されないシフトクロック i に同期して暗号文 C のビット列 C[i] が入力し始めると、シフトアウトからは、乱数 R のビット列 R[i] が出力される。これにより、排他的論理和回路 303 の一方の入力には、R[i] が供給され、排他的論理和回路 303 の他方の入力には、暗号文 C[i] が供給されるので、その出力は、第 1 の暗号化メッセージを復号化した第 1 の領域の通信メッセージ M[i] = R[i] (+) C[i] となる。

【0216】ここで、(+) は排他的論理和演算を示す。この状態は、初期設定された乱数 R の k ビット全てがシフトアウトするまで、即ち $1 \leq i \leq k$ の間継続する。

【0217】次いで、 $i = k + 1$ 以降のシフトクロックにおいては、シフトアウトデータは、シフトインデータの k ビットタイム遅延したデータである C[i - k] となるので、排他的論理和回路 303 の一方の入力には、C[i - k] が供給され、他方の入力には C[i] が供給されるので、その出力は、第 2 の暗号化メッセージを復号化した第 2 の領域の通信メッセージ M[i] = C[i - k] (+) C[i] となる。

【0218】この受信装置 59 によれば、k ビットの乱数 R が初期設定される k ビットシフトレジスタ 301 を用いることにより、シフトアウトデータは、 $R[i] \parallel C[i - k]$ となるので、第 1 及び第 2 の暗号化メッセージに対する処理が自動的に切り替わる。このため、特に第 1 及び第 2 の暗号化メッセージの分離や、通信メッセージの第 1 の領域である先頭ブロックを切り出すことや、第 1 及び第 2 の領域の復号化された通信メッセージを接続する必要がなく、簡単な回路構成で処理速度の高

$$R[n] = h_1 R[n-1] + h_2 R[n-2] + \dots + h_k R[n-k] \pmod{2} \dots (24)$$

式 (24) に示す漸化式により新たな乱数のビット値 R[n] が生成され、シフトインされる。

【0224】この漸化式 (24) によって生成される乱

$$f(x) = 1 + h_1 x + h_2 x^2 + \dots + h_k x^k \dots (25)$$

式 (25) の特性多項式がガロア体 GF(2) 上の原始多項式となることである。

【0225】2 入力排他的論理和回路 303 は、シフトレジスタ 301 b からシフトアウトされる乱数 R[i] または平文 M[i - k] と、平文 M[i] との排他的演算を行

い復号化装置を実現できる。

【0219】なお、図 22 の k ビットシフトレジスタ 301 に k ビットのパラレルロードパスを設けることなく、シフトイン入力の直前に切替器を設けて直列入力により乱数 R を設定してもよい。さらに、k ビットシフトレジスタ 301、または k ビットシフトレジスタ 301 と排他的論理和回路 303 とを含む回路を 1 チップの集積回路に集積化すると、送信装置及び受信装置を小型化できる。

【0220】図 23 は、図 5 中の乱数生成処理部 313 の詳細例である乱数発生器を示すブロック回路図であり、請求項 25 に対応する。送信装置及び受信装置にそれぞれ設けられた乱数発生器 313 は、乱数パラメータとして、乱数発生アルゴリズム H と、乱数初期値 R0 とを受け取り、この乱数パラメータに従って、双方の乱数発生器が互いに等しい乱数を生成させるものである。

【0221】同図において、乱数発生器は、レジスタ 301 a、シフトレジスタ 301 b、アンドゲート 311 a ~ 311 d、排他的論理和回路 313、及び切替器 315 を備えて構成されている。レジスタ 301 a は、最大 k ビットのレジスタであり、乱数発生アルゴリズム H が設定される。シフトレジスタ 301 b は、k ビットのシフトレジスタであり、k ビットの乱数初期値 R0 が初期設定される。

【0222】アンドゲート 311 a ~ 311 d は、最大 k 個の 2 入力アンドゲートであり、レジスタ 301 a とシフトレジスタ 301 b との互に対応するビット同士の論理積を生成し、排他的論理和回路 313 に出力する。排他的論理和回路 313 は、最大 k 個設けられたアンドゲート 311 a ~ 311 d の出力の排他的論理和を生成し、これを切替器 315 を介してシフトレジスタ 301 b のシフトインに供給する。切替器 315 は、スイッチで図示されているが、実際には 1 ビット 2 ウェイセレクタである。

【0223】ところで、レジスタ 301 a に設定される乱数発生アルゴリズム H は、それぞれ 0 または 1 の値をもつ h_i ($1 \leq i \leq k$) からなり、シフトレジスタ 301 b のある時点の k ビットの内容を $R[n-1]$, $R[n-2]$, ..., $R[n-k]$ とすれば、

【数 23】

数が最大周期系列となる必要十分条件は、

【数 24】

ってストリーム暗号化するものである。

【0226】切替器 315 の接点が右側に倒されていると、シフトレジスタ 301 b は乱数発生器として動作し、切替器 315 の接点が左側に倒されると、これ以後シフトレジスタ 301 b は乱数発生器としての動作を停

止し、通信メッセージである平文 $M[i]$ の k ビット遅延回路として動作することとなる。

【0227】これにより通信メッセージの第1の領域においては、乱数 $R[i]$ と平文 $M[i]$ との排他的演算が行われ、暗号文 $C[i] \equiv R[i](+)M[i]$ が得られる。また、切替器315を左側に倒してから k ビットタイム後には、通信メッセージの第2の領域の暗号化である暗号文 $C[i] \equiv M[i-k](+)M[i]$ が得られる。

【0228】なお、本実施の形態において、乱数発生アルゴリズムHが設定されるレジスタ301a及びアンドゲート311は、必ずしも k ビット相当の個数を必要とせず、選択される乱数発生アルゴリズム間で共通に0の値をとる h_i に対応するビットは、レジスタ301a及びアンドゲート311を省略することができる。

【0229】また、本実施の形態は、共有乱数の値自体を送信装置から受信装置へ送る代わりに、乱数発生アルゴリズム及び乱数初期値を送ることにより、双方で同一の乱数を発生するので、十分長い乱数も少ない情報で共有することができる。さらに、切替器315の切替タイミングは、特に限定されることがないので、乱数発生器と乱数発生アルゴリズムによって定まる周期を超えて乱数を利用することも可能となり、通信メッセージ全体を第1の領域として、 $C[i] \equiv R[i](+)M[i]$ により暗号化することもできる。

【0230】さらに、本実施の形態の変形として、乱数発生アルゴリズムまたは乱数初期値のいずれか一方だけを送信装置から受信装置へ秘密に送ることにより、両方で乱数を共有することもできる。乱数発生初期値のみを送る場合には、レジスタ301a及びアンドゲート311を省略し、シフトレジスタ301bから排他的論理和回路303へ直接結線すればよい。

【0231】図24は、図6に示した後続ブロック暗号化処理部(a)および後続ブロック復号化処理部(b)の構成例を示す第11実施形態を示す回路図である。

【0232】図24(a)において、後続ブロック暗号化処理部151は、 k ビットシフトレジスタ301と、排他的論理和回路303とを備えて構成されている。 k ビットシフトレジスタ301のシフトイン入力には、先頭ブロック切り出し処理部111からビット直列に供給される通信メッセージの第2の領域である平文 M の後続ブロック $M[i]$ ($k < i \leq N$)の信号が接続され、シフトアウト出力には、排他的論理和回路303の一方の入力が接続されている。排他的論理和回路303の他方の入力には、平文 $M[i]$ ($k < i \leq N$)の信号が接続されている。排他的論理和回路303の出力は、暗号文直接処理部174へ接続されている。

【0233】次に、この後続ブロック暗号化処理部151の動作を説明する。まず最初に、 k ビットシフトレジスタ301には、例えば k ビットのパラレルロードパスから k ビットの通信メッセージの第1の領域である平文

の先頭ブロック $M_{1,k}$ が設定される。次いで、図示されないシフトクロック i に同期して平文 M の後続ブロックのビット列 $M[i]$ が入力し始めると、シフトアウトからは、平文 M の先頭ブロックのビット列 $M[i-k]$ が出力される。これにより、排他的論理和回路303の一方の入力には、 $M[i-k]$ が供給され、排他的論理和回路303の他方の入力には、平文 $M[i]$ が供給されるので、その出力は、第2の暗号化メッセージ $C[i] = M[i-k](+)M[i]$ となる。

【0234】図24(b)において、後続ブロック復号化処理部251は、 k ビットシフトレジスタ301と、排他的論理和回路303とを備えて構成されている。

【0235】暗号文分離処理部274から出力される第2の暗号文のビット列 $C[i]$ ($k < i \leq N$)は、 k ビットシフトレジスタ301のシフトイン入力に接続されている。シフトアウト出力には、排他的論理和回路303の一方の入力が接続され、303の他方の入力には、暗号文 $C[i]$ ($k < i \leq N$)の信号が接続されている。排他的論理和回路303の出力は、平文のビット列 $M[i]$ ($k < i \leq N$)を出力する。

【0236】次に、この後続ブロック復号化処理部251の動作を説明する。まず最初に、 k ビットシフトレジスタ301には、例えば k ビットのパラレルロードパスから k ビットの通信メッセージの第1の領域である平文の先頭ブロック $M_{1,k}$ が設定される。次いで、図示されないシフトクロック i に同期して暗号文 C の後続ブロックのビット列 $C[i]$ が入力し始めると、シフトアウトからは、平文 M の先頭ブロックのビット列 $M[i-k]$ が出力される。これにより、排他的論理和回路303の一方の入力には、 $M[i-k]$ が供給され、排他的論理和回路303の他方の入力には、暗号文 $C[i]$ が供給されるので、その出力は、第2の暗号化メッセージを復号化した第2の領域の通信メッセージ $M[i] = M[i-k](+)C[i]$ となる。

【0237】図25は、 k ビット並列にストリーム暗号化を行う送信パイプライン(a)及び k ビット並列にストリーム暗号の復号化を行う受信パイプライン(b)の構成を示すブロック図であり、請求項29に対応する。

【0238】同図(a)において、送信パイプラインは、Aレジスタ401、2ウェイセクタ403、Bレジスタ405、並列排他的論理和回路407、及び k ビット送信回路409を備えて構成されている。これらの構成要素のデータパスは全て k ビットの幅を有する。

【0239】送信パイプラインの動作は、以下の通りである。まず、セクタ403で k ビット並列の乱数 R を選択し、これをBレジスタ405にセットする。これ以後はセクタ403はAレジスタ401を選択する。次いで、平文 M が k ビット単位でAレジスタに供給される。並列排他的論理和回路407は、Aレジスタ401の内容と、Bレジスタ405の内容とをそれぞれビット

毎に排他的論理和演算を行い、kビット送信回路409へ出力する。

【0240】かくして、平文Mの最初のkビットのブロックM1は、 $C1 = R(+)M1$ により並列に暗号化され、平文Mの最初のブロックM1以外のkビットのブロックMjは、 $Cj = Mj-1(+)Mj$ により並列に暗号化される。

【0241】同図(b)において、受信パイプラインは、kビット受信回路411、Aレジスタ401、2ウェイセレクタ403、Bレジスタ405、及び並列排他的論理和回路407を備えて構成されている。これらの構成要素のデータパスは全てkビットの幅を有する。

【0242】受信パイプラインの動作は、以下の通りである。まず、セレクタ403でkビット並列の乱数Rを選択し、これをBレジスタ405にセットする。これ以後はセレクタ403はAレジスタ401を選択する。次いで、kビット受信回路より暗号文Cがkビット単位でAレジスタに供給される。並列排他的論理和回路407は、Aレジスタ401の内容と、Bレジスタ405の内容とをそれぞれビット毎に排他的論理和演算を行い、k

【0243】かくして、暗号文Cの最初のkビットのブ

$$M = 10100001111100000 \quad (26)$$

$$M' = \# \# \# 10100001111100 \quad (27)$$

$$C = ***10101110011100 \quad (28)$$

こうして得られたCから、元のビット列Mを推測する方法はない。排他的論理和をとったあとの、iビット目は、 $M[i](+)M[i-k]$ となり、また $i \pm k$ ビット目は、それぞれ、 $M[i+k](+)M[i]$ 、 $M[i-k](+)M[i-2k]$ となるが、これらの値からM[i]を得る関係式は存在しない。

【0247】

【発明の効果】以上説明したように、本発明によれば、従来の秘密鍵暗号の鍵配送問題を解決し、少量の秘密鍵の配送だけで、大量の通信メッセージの秘密鍵暗号による通信を可能とするという効果がある。

【0248】また本発明によれば、従来の秘密鍵暗号あるいは公開鍵暗号と同等の安全性を確保しつつ高速な暗号通信を行うことができるという効果がある。

【0249】また本発明によれば、従来型の秘密鍵暗号や公開鍵暗号と比べて、暗号化および復号化の処理量が大幅に削減され、画像や音声を含むリアルタイム性のあるマルチメディア情報の秘密通信に適用可能な暗号を用いた通信システムを提供することができるという効果がある。

【0250】マルチメディアかつリアルタイム情報の具体例としては、テレビ会議など多量のデータが長時間継続するような場合を挙げることができる。本方式は、公衆網やインターネット上での暗号化テレビ会議に利用することができる。主要な処理は、オリジナルメッセージ

ロックC1は、 $M1 = R(+)C1$ により並列に復号化され、暗号文Cの最初のブロックC1以外のkビットのブロックCjは、 $Mj = Mj-1(+)Cj$ により並列に復号化される。

【0244】次に、本発明に係るストリーム暗号による通信方式における安全強度を考察する。本発明のストリーム暗号方式においては、秘密鍵である乱数または通信メッセージの第1の領域である公開鍵暗号化される部分は、使用する公開鍵暗号の安全強度によって評価することができる。通信メッセージ部分または通信メッセージの第2の領域である排他的論理和部分の安全強度を考察する。

【0245】この問題は、次の問題に言い換えることができる。つまり、あるビット列Mを考える。例えば、 $M = 10100001111100000$ とする。Mをkビット分右シフトして、先頭のkビットは乱数ビット列R(#, #, ..., #)で補い最後のkビットは削除することにより作ったビット列をM'とする。MとM'とのビット毎の排他的論理和をとり、暗号ビット列 $C = M(+)M'$ を得る。以下には、 $k = 3$ とした場合を示す。

【0246】

【数25】

と、その定数ビットだけ右シフトしたメッセージとの排他的論理和演算であり、メッセージが不定長であるようなストリーム型のリアルタイム情報の暗号通信には特に有効である。

【0251】また大量データのファイルを暗号化転送するときにも、暗号化および復号化の処理量の少ない本発明方式は極めて有効である。

【0252】さらに本発明によれば、暗号化及び復号化の処理をさらに高速化するために、並列処理が可能であり、またハードウェア化が容易であるストリーム暗号を用いた通信システムを提供することができるという効果がある。

【図面の簡単な説明】

【図1】本発明に係るストリーム暗号による通信システムの第1実施形態を示すブロック図である。

【図2】本発明に係るストリーム暗号による通信システムの第3実施形態を示すブロック図である。

【図3】本発明に係るストリーム暗号による通信システムの第4実施形態を示すブロック図である。

【図4】本発明に係るストリーム暗号による通信システムの第5実施形態を示すブロック図である。

【図5】本発明に係るストリーム暗号による通信システムの第6実施形態を示すブロック図である。

【図6】本発明に係るストリーム暗号による通信システムの第7実施形態を示すブロック図である。

【図 7】本発明に係るストリーム暗号による通信システムの第 8 実施形態を示すブロック図である。

【図 8】本発明に係るストリーム暗号による通信システムの第 9 実施形態を示すブロック図である。

【図 9】本発明に係るストリーム暗号による通信システムの第 1 実施形態の暗号化送信動作を説明するフローチャート図である。

【図 10】本発明に係るストリーム暗号による通信システムの第 1 実施形態の受信復号化動作を説明するフローチャート図である。

【図 11】本発明に係るストリーム暗号による通信システムの第 3 実施形態の暗号化送信動作を説明するフローチャート図である。

【図 12】本発明に係るストリーム暗号による通信システムの第 3 実施形態の受信復号化動作を説明するフローチャート図である。

【図 13】本発明に係るストリーム暗号による通信システムの第 5 実施形態の暗号化送信動作を説明するフローチャート図である。

【図 14】本発明に係るストリーム暗号による通信システムの第 5 実施形態の受信復号化動作を説明するフローチャート図である。

【図 15】本発明に係るストリーム暗号による通信システムの第 6 実施形態の乱数共有化処理動作を説明するフローチャート図である。

【図 16】本発明に係るストリーム暗号による通信システムの第 7 実施形態の暗号化送信動作を説明するフローチャート図である。

【図 17】本発明に係るストリーム暗号による通信システムの第 7 実施形態の受信復号化動作を説明するフローチャート図である。

【図 18】本発明に係るストリーム暗号による通信システムの第 8 実施形態の暗号化送信動作を説明するフロー

チャート図である。

【図 19】本発明に係るストリーム暗号による通信システムの第 8 実施形態の受信復号化動作を説明するフローチャート図である。

【図 20】本発明に係るストリーム暗号による通信システムの第 9 実施形態の暗号化送信動作を説明するフローチャート図である。

【図 21】本発明に係るストリーム暗号による通信システムの第 9 実施形態の受信復号化動作を説明するフローチャート図である。

【図 22】本発明に係るストリーム暗号による通信システムを構成する送信装置 (a) 及び受信装置 (b) の第 10 実施形態を示すブロック図である。

【図 23】乱数発生アルゴリズム及び乱数初期値を設定可能な乱数発生器の構成を示す回路図である。

【図 24】通信メッセージの先頭ブロックをパッドとする通信システムにシフトレジスタを用いた送信装置 (a) 及び受信装置 (b) の第 11 実施形態を示すブロック図である。

【図 25】k ビット並列に暗号化を行う送信パイプライン処理回路 (a) 及び k ビット並列に復号化を行う受信パイプライン処理回路 (b) である。

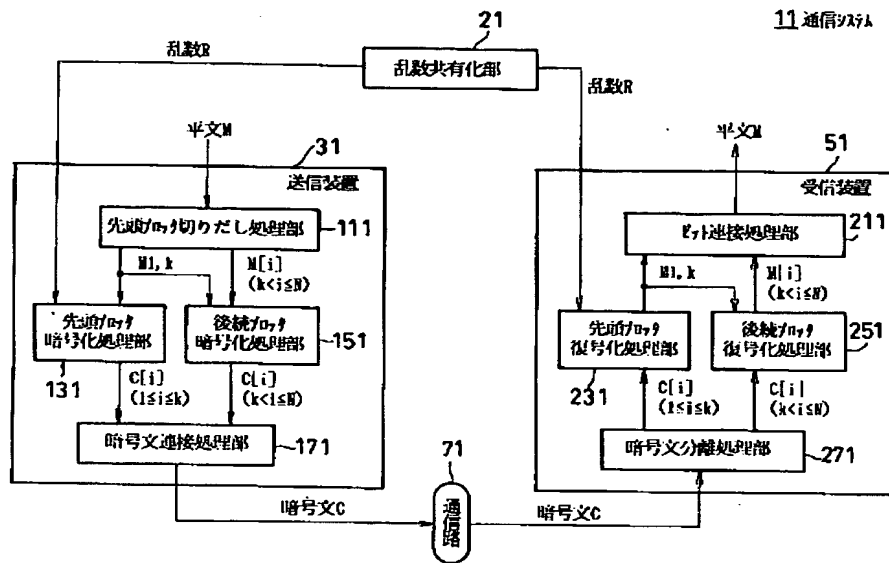
【図 26】従来のバーナム暗号による通信システムの構成を示すブロック図である。

【図 27】DH 型公開鍵配送法を説明する図である。

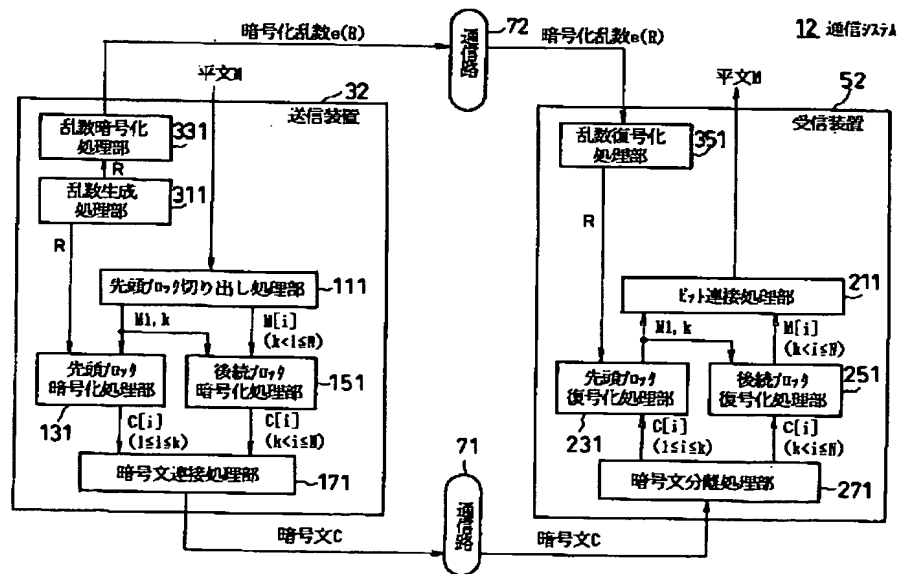
【符号の説明】

11…通信システム、21…乱数共有化部、31…送信装置、51…受信装置、71…通信路、111…先頭ブロック切り出し処理部、131…先頭ブロック暗号化処理部、151…後続ブロック暗号化処理部、171…暗号文連接処理部、211…ビット連接処理部、231…先頭ブロック復号化処理部、251…後続ブロック復号化処理部、271…暗号文分離処理部。

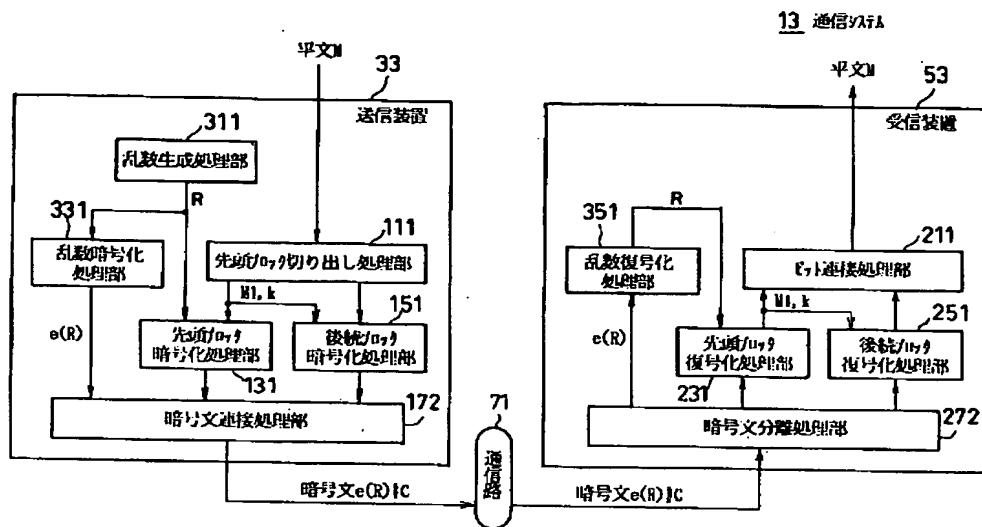
【図1】



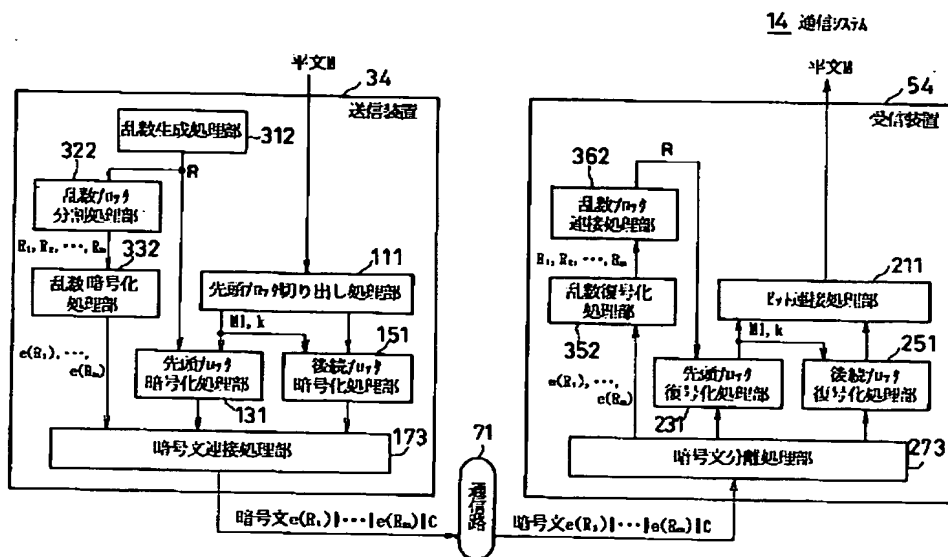
【図2】



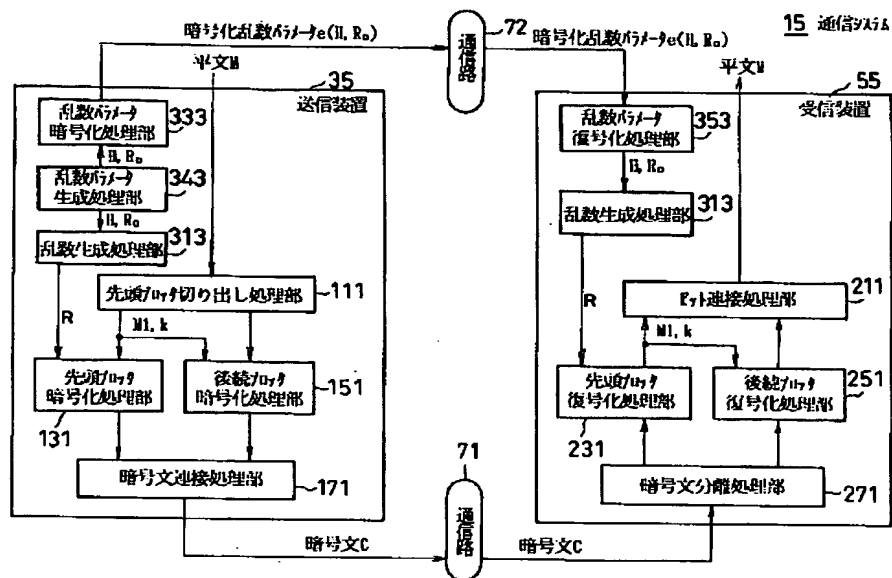
【図 3】



【図 4】

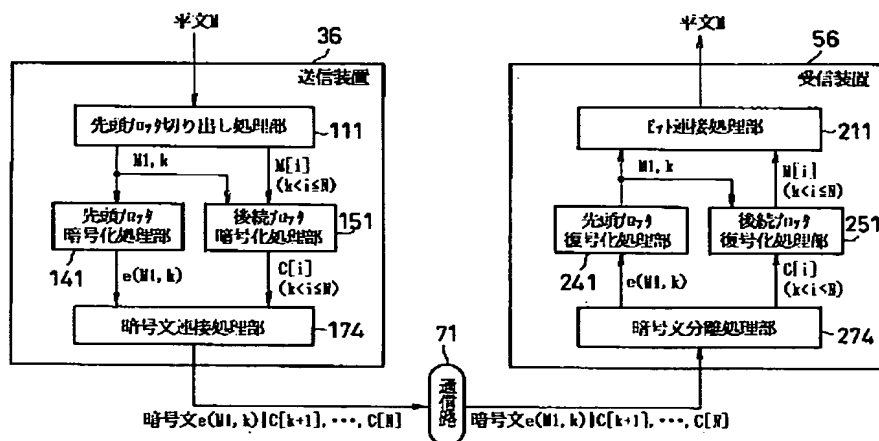


【図5】

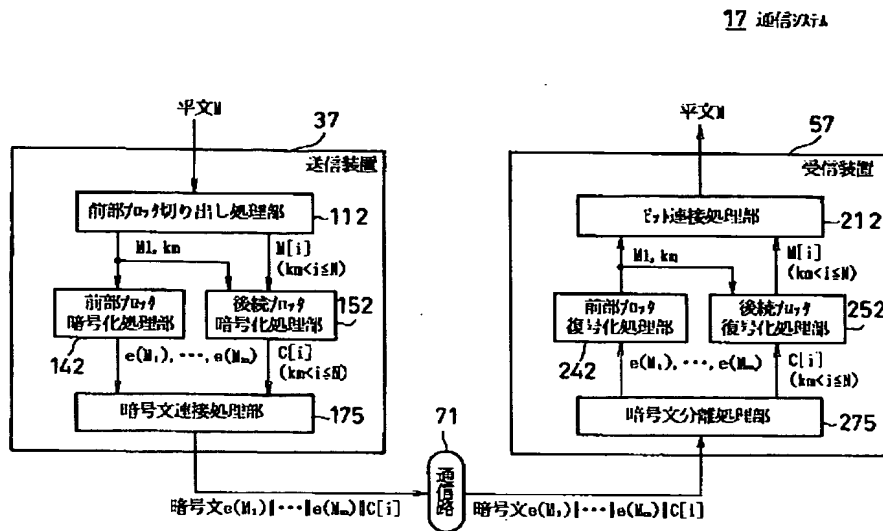


【図6】

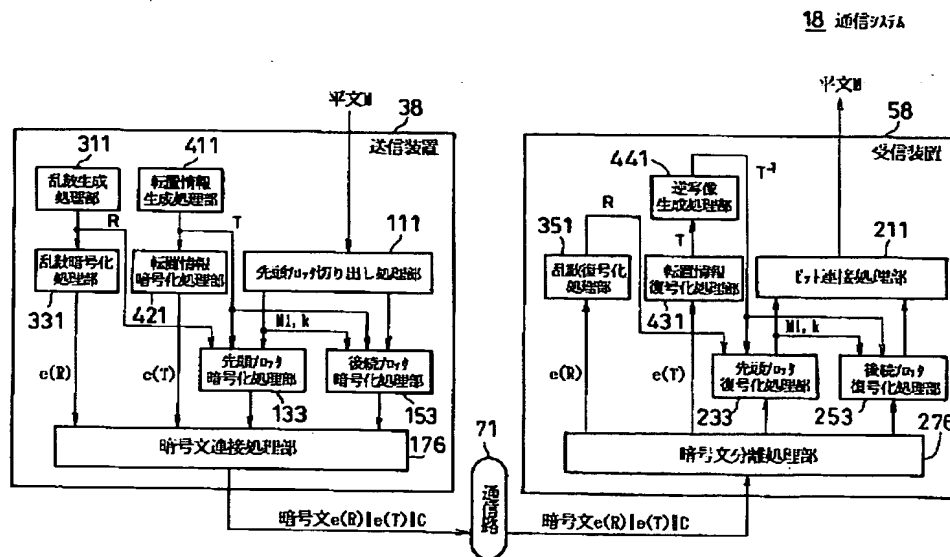
16 通信システム



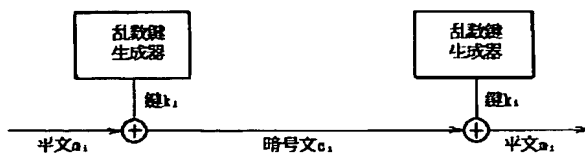
【図7】



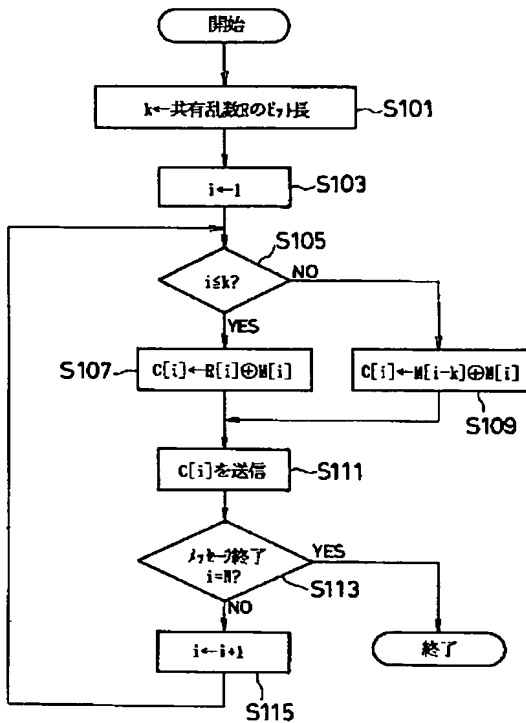
【図8】



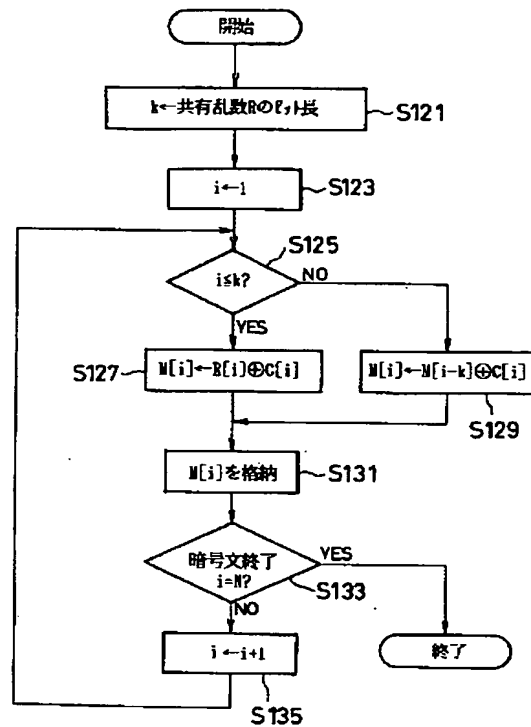
【図26】



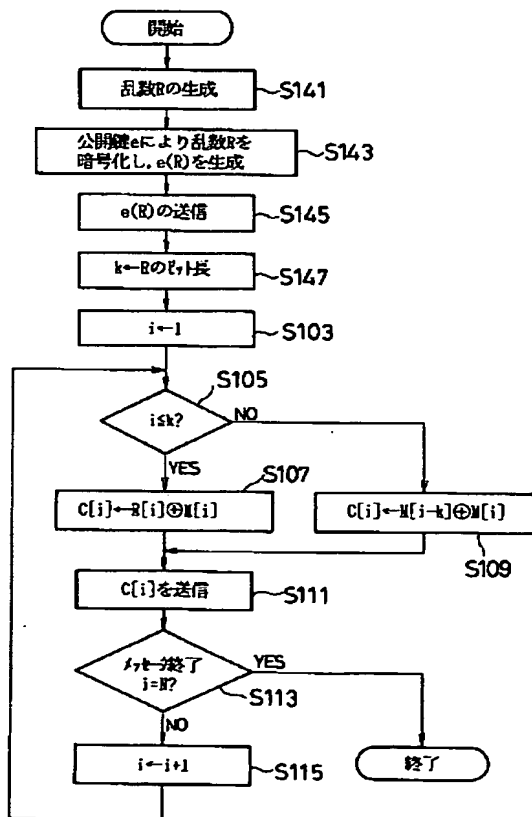
【図9】



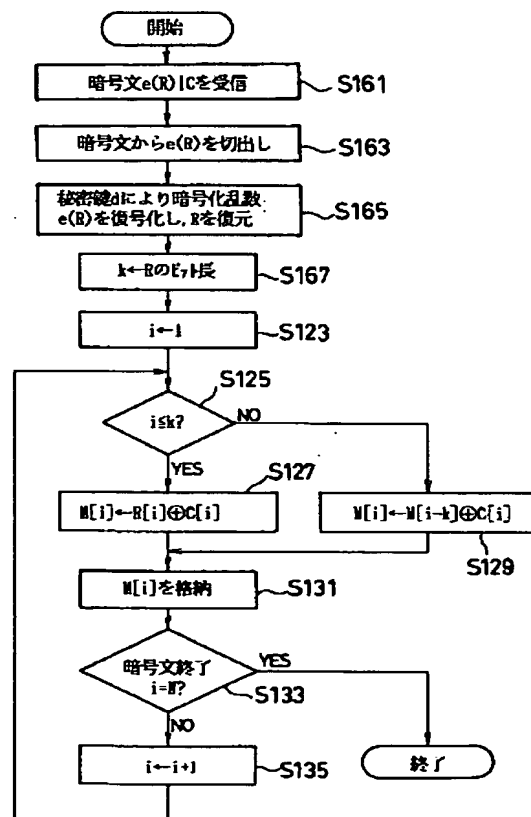
【図10】



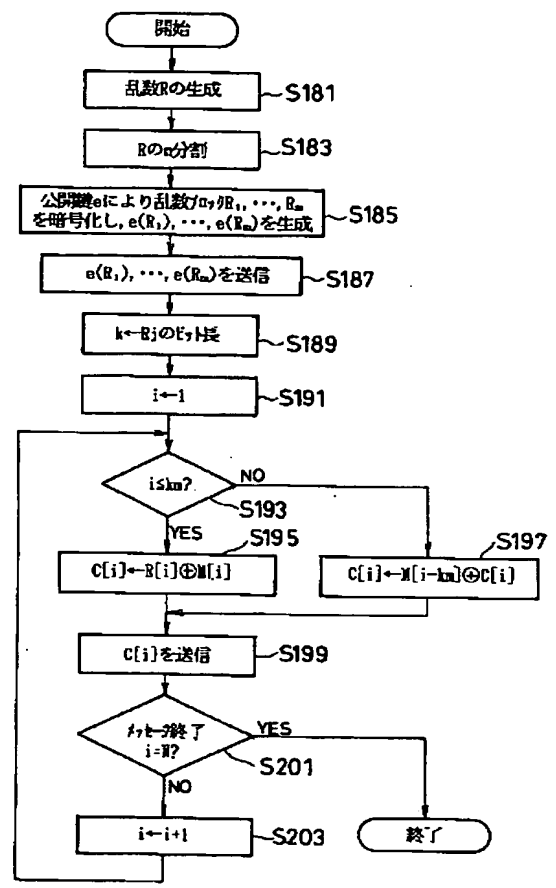
【図11】



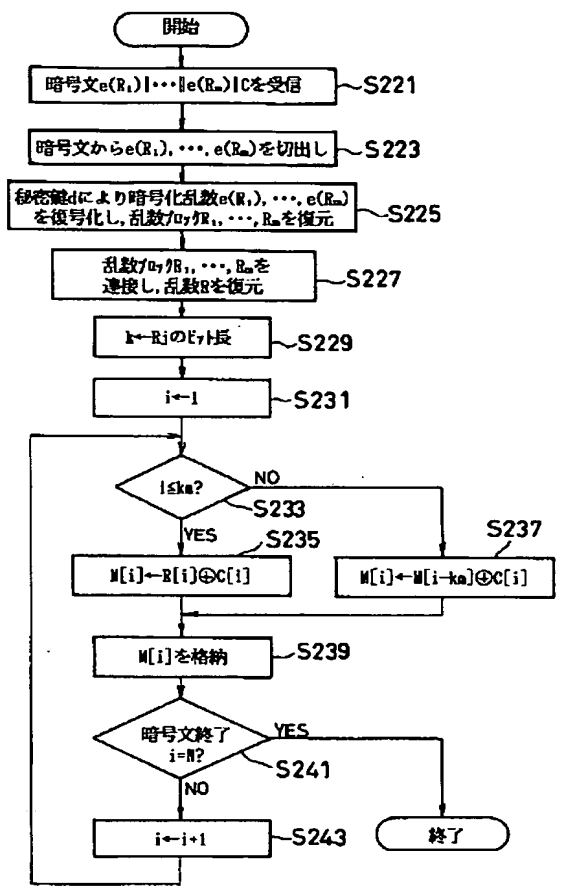
【図12】



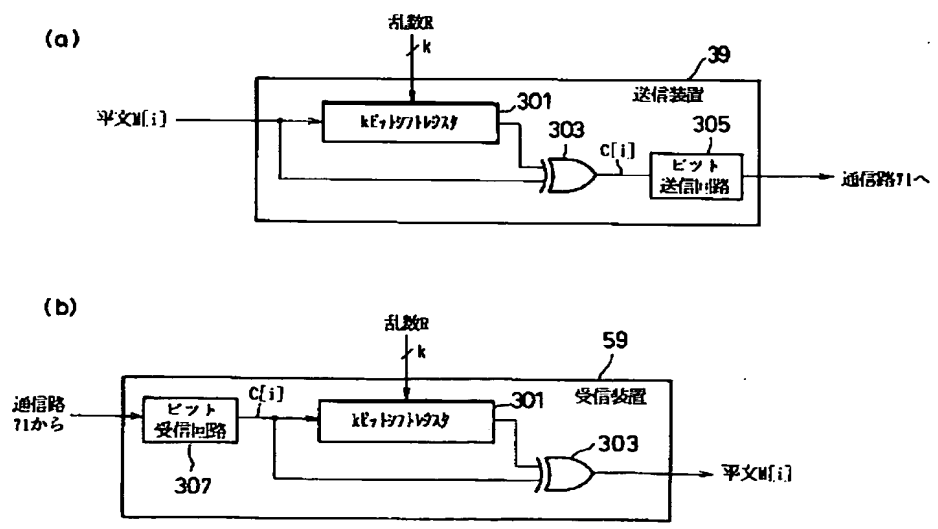
【図 1 3】



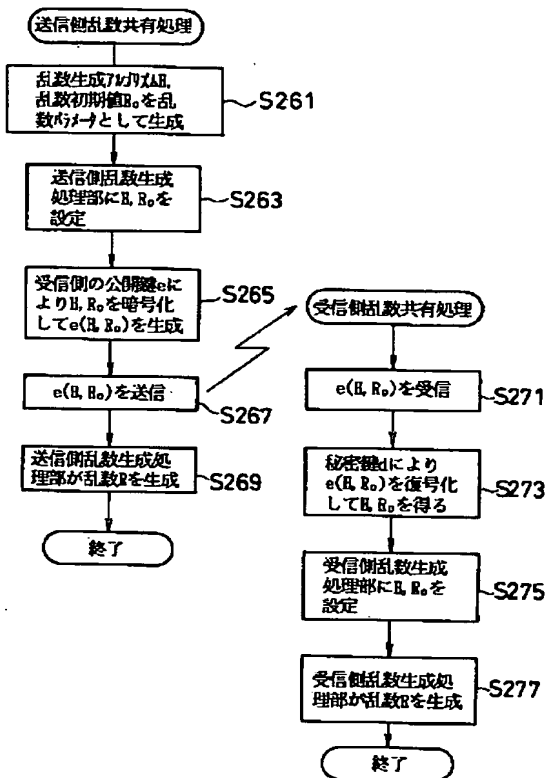
【図 1 4】



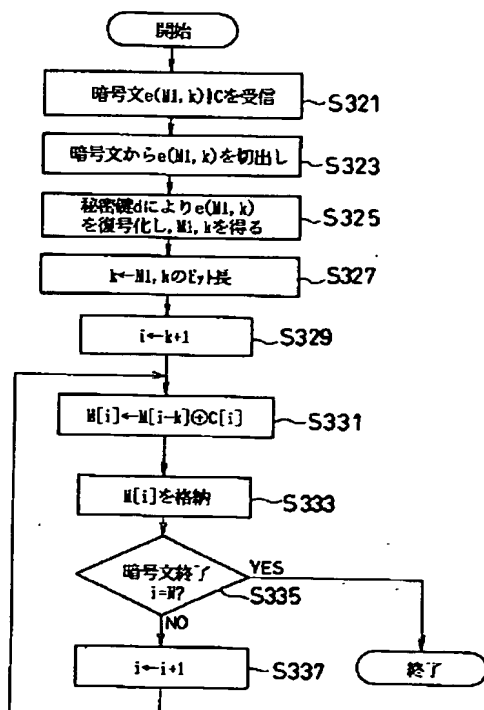
【図 2 2】



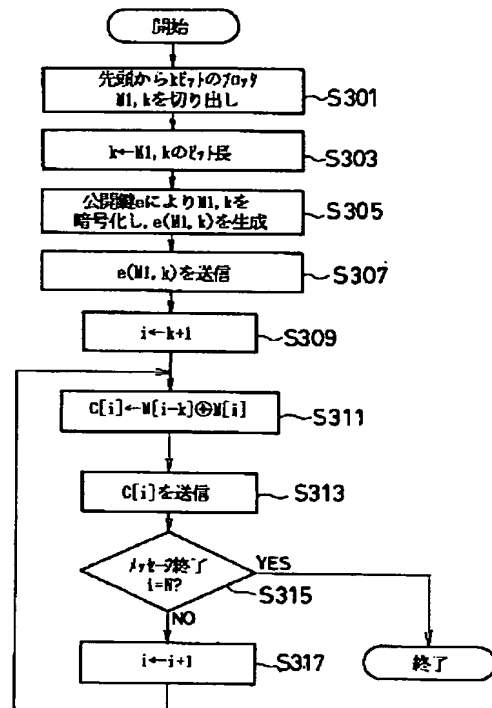
【図 15】



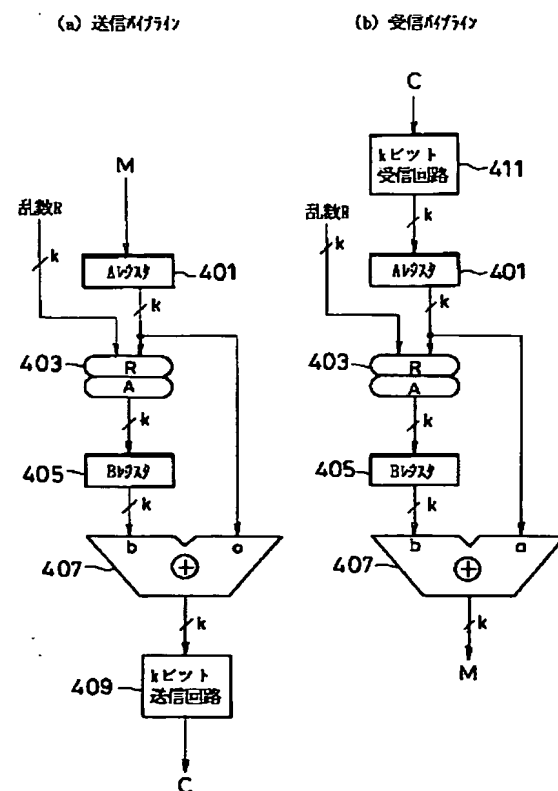
【圖 17】



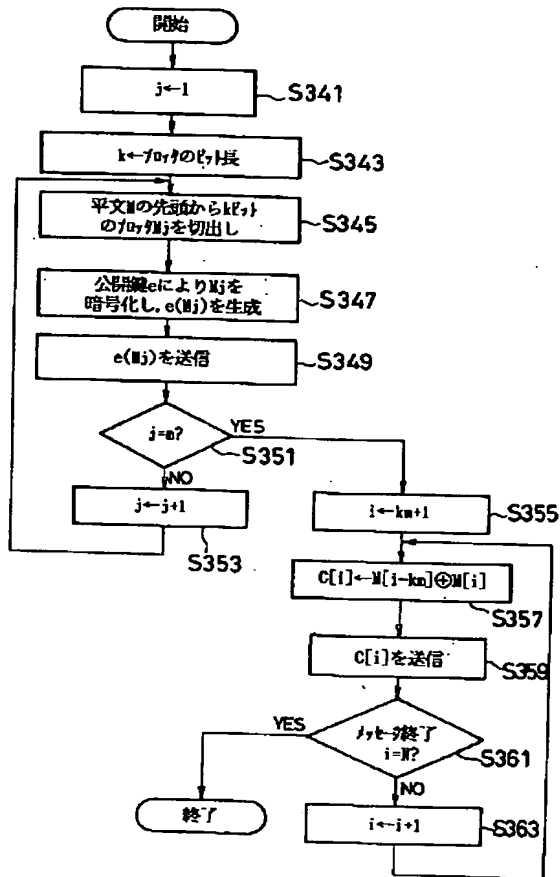
【图 16】



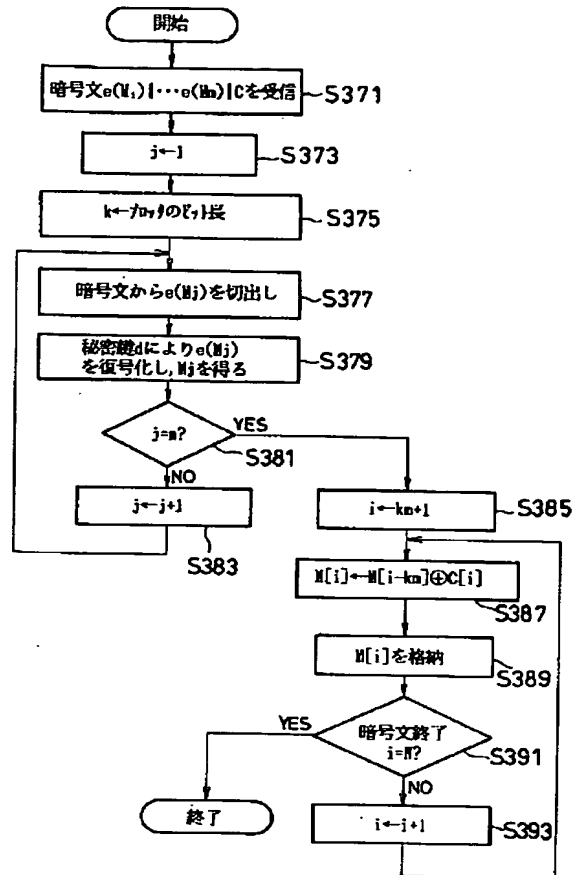
【図 25】



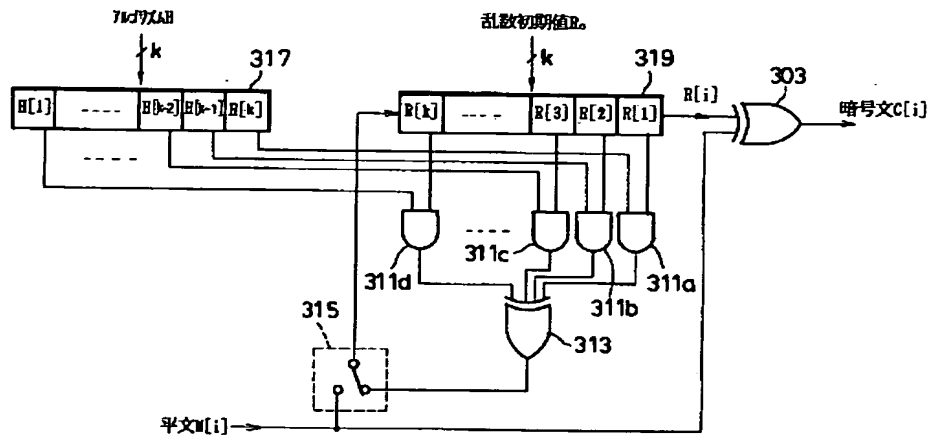
【図18】



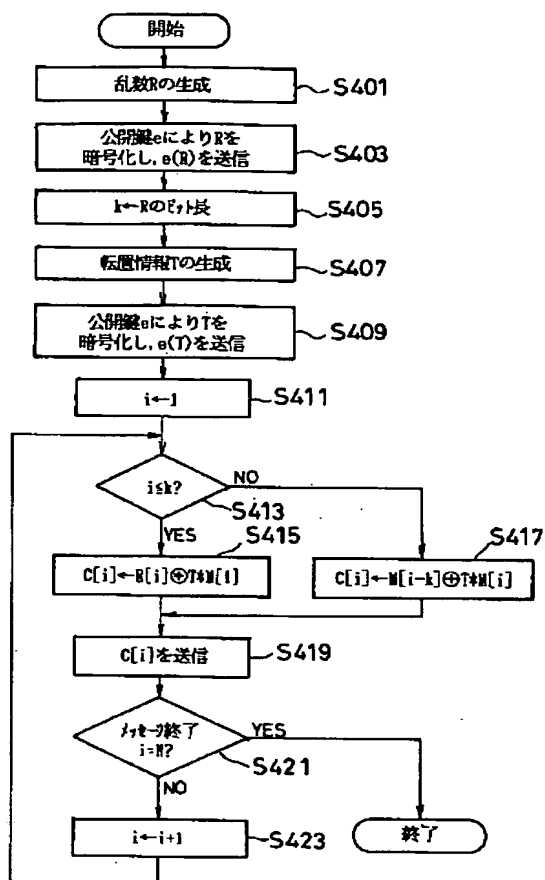
【図19】



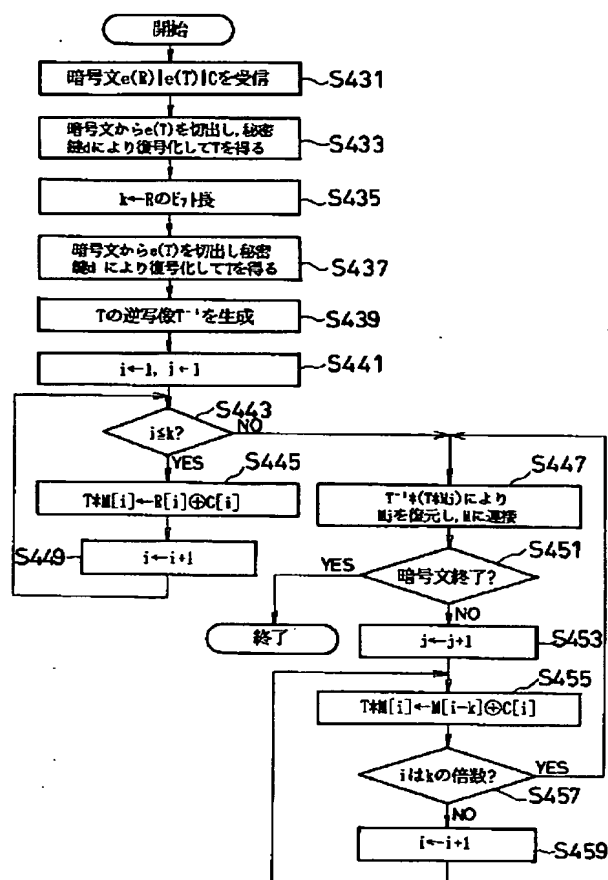
【図23】



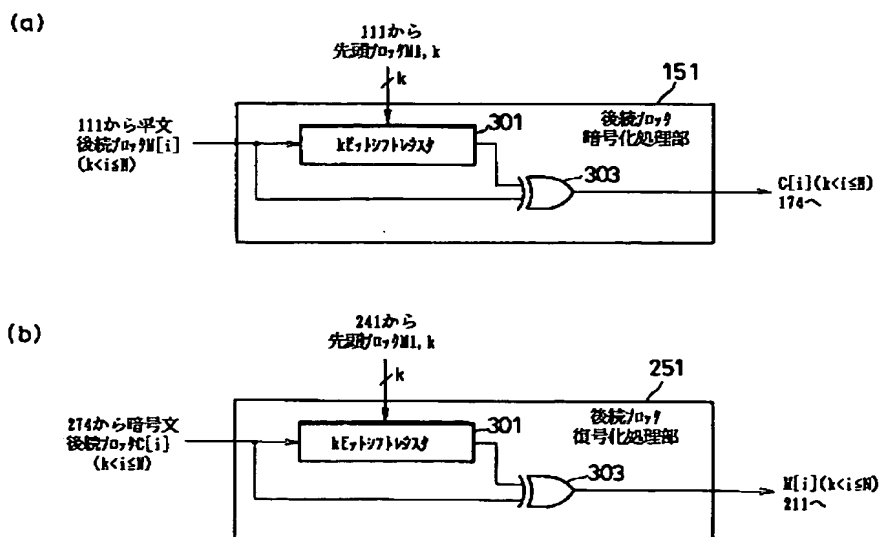
【図 20】



【図 2 1】



【図 24】



【図 27】

